

About Parker vectors and related topics

Daniele A. Gewurz

Contents

| | |
|--|-----------|
| Introduction | 3 |
| 0 Preliminaries | 6 |
| 1 Parker vectors | 10 |
| 1.1 Why we are interested in Parker vectors | 10 |
| 1.2 Definition, first properties and Parker's Lemma | 11 |
| 1.3 Parker vectors and multiple transitivity | 20 |
| 1.4 A possible generalisation | 24 |
| 2 Parker vectors of regular and Frobenius groups | 29 |
| 2.1 Regular groups | 29 |
| 2.2 Relationship between the Parker vector of G and the Parker vector of G_α | 32 |
| 2.3 Frobenius groups | 34 |
| 3 Permutation groups with a regular normal subgroup and their Parker vectors | 41 |
| 3.1 Permutation groups with a regular subgroup | 41 |

| | | |
|----------|--|-----------|
| 3.2 | The case of the normal regular subgroup | 42 |
| 4 | Pólya enumeration | 48 |
| 4.1 | Cycle index and Pólya's theory | 48 |
| 4.2 | Links with Parker vectors | 52 |
| 4.3 | Vector space cycle index and vector space Parker vectors . . . | 56 |
| 5 | Linear and affine groups | 61 |
| 5.1 | Parker vectors of general linear groups | 62 |
| 5.2 | Parker vectors of other linear and affine groups | 68 |
| A | GAP programs and a table of Parker vectors | 73 |
| | Bibliography | 84 |

Introduction

*Non domandarci la formula che mondi possa aprirti,
sì qualche storta sillaba e secca come un ramo.*

Eugenio Montale

*(Don't ask of us the formula which can open whole worlds for you,
but rather some crooked syllable, dried as a branch.*

Transl. G. Almansi and B. Merry [AM77])

This thesis is about Parker vectors. The Parker vector of a finite permutation group G is a finite sequence of nonnegative integers connected with the action by conjugation of G on the set of cycles appearing in its elements.

The main themes in this thesis are to understand what information about the group can be recovered from so little data, and to obtain more or less explicitly the Parker vectors of several important classes of groups.

After a preliminary chapter recalling some standard definitions and results, in Chapter 1 we give the definition and generalities about Parker vectors. We begin by giving, by way of motivation for their study, the application in computational Galois theory from which they arose. Then we give the definition and the fundamental result, Parker's lemma, relating the Parker vector of a group to the cycle structure of its elements. Other results about Parker vectors are then given, relating them to some properties of permutation groups, such as transitivity and multiple transitivity, leading to

the characterisation of the symmetric and alternating groups through their Parker vectors. The relationship between the Parker vector of a group and its permutation character suggests a generalisation to any character.

In chapter 2 we examine regular and Frobenius groups, the structure of which allows us to give an explicit description of their Parker vectors. Further, we find the relationships between the Parker vector of a group G and that of its point stabiliser G_α .

Abstracting one of the peculiar properties of Frobenius groups, their having a regular normal subgroup, leads to investigating what can be said in general about permutation groups admitting such a subgroup, in chapter 3.

In chapter 4 we show how the cycle index of a permutation group (central in Pólya enumeration theory) is a very powerful tool when investigating Parker vectors. A key result links the cycle index of a permutation group to its Parker vector, allowing us to use standard results about the former to get new insights into the latter, such as its behaviour with respect to direct and wreath products. The last section of this chapter introduces a tentative extension to linear groups of the concept of Parker vector, following an analogous extension of cycle indices.

The affine general groups are particular cases of the class of groups with a regular normal subgroup. The problem of determining their Parker vectors, as well as those of the general and special linear groups, is tackled and solved in the last chapter, where explicit representatives are also shown for the orbits counted by the vectors.

This work closes with an appendix containing some GAP routines useful in studying Parker vectors (but that have not been used to get the results in the thesis), and a table, obtained using them, with the Parker vectors of all transitive permutation groups of degree up to 10.

I am deeply indebted to Prof. Peter J. Cameron for having patiently advised me throughout my work, pointing out to me the very subject of Parker vectors, suggesting me continuously new ways of looking at them, and accepting me as a visitor at the School of Mathematical Sciences of Queen Mary and Westfield College in London.

I am also very grateful to Prof. Marialuisa J. de Resmini for her suggestions and encouragement.

Chapter 0

Preliminaries

In this chapter we shall just fix the notation and the definitions of standard concepts we are going to use, excluding more specific concepts that are going to be used in just a section, and which will be defined there.

Permutations and other actions By a *permutation group* of degree n we mean, as usual, a subgroup G of S_n , the symmetric group on n points, or a group G' acting in an equivalent way to such a subgroup; that is, there are an isomorphism $\varphi : G \rightarrow G'$ and a bijection $f : \{1, 2, \dots, n\} \rightarrow \Delta$, where Δ is the set on which G' acts, such that for all $g \in G$, $\alpha \in \{1, 2, \dots, n\}$,

$$\alpha^g f = (\alpha f)^{g\varphi}.$$

As shown, we shall write the point obtained by acting on α with $g \in G$, as α^g . Also, we shall put maps or acting elements of a group on the right of their argument. So, permutations compose from left to right (for instance, $(12)(13) = (123)$); analogously, the vector obtained from v by acting on it with the matrix A is vA , so that $(vA)B = v(AB)$ (for instance, $(1, 0) \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = (1, 2)$).

Let us recall that a permutation group G (or its action) is called *transitive* when it has exactly one orbit (that is, for all $\alpha, \beta \in \Delta$, $g \in G$ exists such that $\alpha^g = \beta$); it is called *n-transitive* when, for any two n -tuples of distinct points of Δ , $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$, there exists an element g of G such that $\alpha_i = \beta_i$ for $i = 1, 2, \dots, n$. So, 1-transitivity is transitivity, whereas n -transitivity for $n \geq 2$ is generically referred to as *multiple transitivity*. There are very strict limits to high multiple transitivity: the only groups that are n -transitive for $n \geq 6$ are S_m and A_{m+2} (the alternating group on $n + 2$ points), with $m \geq n$; the only non-trivial 4-transitive groups are Mathieu groups M_{11} and M_{23} , the only non-trivial 5-transitive ones are M_{12} and M_{24} .

Further, a permutation group is *primitive* if it has no non-trivial blocks, where a *block* is a subset Γ of Δ such that, for all $g \in G$, $\Gamma \cap \Gamma^g = \Gamma$ or $\Gamma \cap \Gamma^g = \emptyset$; the trivial blocks are \emptyset , the singletons $\{\alpha\}$ ($\alpha \in \Delta$), and Δ . This definition is equivalent to saying that all stabilisers G_α are maximal subgroups. It is straightforward to show that a 2-transitive group is primitive.

For the definitions of semiregularity and regularity, and of Frobenius groups, we refer to the beginning of the relevant sections (2.1 and 2.3, respectively).

Products of permutation groups The direct product of two permutation groups G and H , acting on the sets Ω and Δ respectively, induces in a natural way actions on the disjoint union $\Omega \dot{\cup} \Delta$ and on the cartesian product $\Omega \times \Delta$.

The first one is obviously given by

$$\alpha^{(g,h)} := \begin{cases} \alpha^g & \alpha \in \Omega \\ \alpha^h & \alpha \in \Delta \end{cases} ;$$

the second one, not less obviously, by $(\alpha, \beta)^{(g,h)} := (\alpha^g, \beta^h)$.

The importance of the first of these constructions lies in the fact that any intransitive group G can be embedded in a direct product of transitive groups, the groups induced by G on its orbits. These transitive groups are called *transitive constituents* of G ; a subgroup of a direct product which projects onto its factors is called a *subcartesian product* of its factors. Thus, any permutation group is a subcartesian product of its transitive constituents.

Let us quickly recall the definition of *wreath product*. If G and H are as above, with H acting on $\Delta = \{1, 2, \dots, m\}$, then their wreath product is the semidirect product of G^m (direct product of G by itself m times) by H , where H acts on G^m by $(g_1, \dots, g_m)^h := (g_{1^{h^{-1}}}, \dots, g_{m^{h^{-1}}})$. It is denoted by $G \wr H$ (or $G \text{ wr } H$), and $|G \wr H| = |G|^m |H|$. There are two somehow “natural” actions induced by $G \wr H$, an imprimitive one and a possibly primitive one.

The first one is defined on $\Omega \times \Delta$ by

$$(\omega, \alpha)^{(g_1, g_2, \dots, g_m, h)} := (\omega^{g_\alpha}, \alpha^h);$$

a system of blocks (i.e. a set consisting of a block and its translates) for this action is given by $\{\Omega \times \{\alpha\} : \alpha \in \Delta\}$. This action is important because it gives a sort of “universal” imprimitive group. More precisely, given a transitive imprimitive group K , if Ω is a non-trivial block for its action, Δ is the set of translates of Ω , G is the group induced on Ω by its setwise

stabiliser, and H is the group induced on Δ by K , then K can be embedded into $G \wr H$ in its action on the set $\Omega \times \Delta$ which can be identified with the set on which K acts. By iterating this construction, one gets a set of primitive groups, the *primitive components* of K , in a suitable wreath product of which K can be embedded. Unfortunately, the primitive components, unlike the transitive constituents, are not uniquely determined.

The second action of $G \wr H$, called *product action*, is defined on Ω^Δ (the set of maps $\Delta \rightarrow \Omega$); if φ is an element of Ω^Δ , the action is given by

$$\varphi^{(g_1, g_2, \dots, g_m, h)}(\alpha) := (\varphi(\alpha^{h^{-1}}))^{g_{\alpha^{h^{-1}}}}.$$

Notation for particular families of groups As usual, we shall denote by C_n the cyclic group of order n ; we shall always consider it as a permutation group in its regular action, in which it can be seen as being generated by a cycle $(12 \dots n)$. The dihedral group of order $2n$ (consisting of the symmetries of the regular n -gon) will be seen as a permutation group on the n vertices and denoted by D_n .

$GL(n, q)$, $AGL(n, q)$, and $SL(n, q)$, where q is a prime power, have the usual meaning.

Main references The results used but not explicitly quoted or proved (such as standard properties of groups and fields) can be found in most texts on algebra, group theory, and permutation groups. The ones I have mostly consulted are [La93], [Ro78], [Wi64], [DM96], and [Ca98].

Chapter 1

Parker vectors

1.1 Why we are interested in Parker vectors

The motivation for studying Parker vectors comes from computational Galois theory. In this context, we can be able to compute (or approximate) the Parker vector of the Galois group of a polynomial, so that it is interesting to understand the amount of information it gives on the group itself.

More precisely, let f be a polynomial of degree n with coefficients in \mathbf{Q} or, without loss of generality, in \mathbf{Z} . We consider the problem of determining G , the Galois group of f over \mathbf{Q} (that is, the Galois group of a splitting field of f , regarded as an extension of \mathbf{Q}). This group permutes the roots of f ; thus it is isomorphic to a subgroup of S_n .

Consider a “sufficiently large” prime p (so that it does not divide the discriminant and the leading coefficient of f). We reduce f modulo p , obtaining a polynomial $\bar{f} \in GF(p)[x]$. Let $K = GF(p^k)$ be the splitting field of \bar{f} and $\vartheta : a \mapsto a^p$ its Frobenius automorphism. Then ϑ permutes the roots of \bar{f} , and the cycle lengths of ϑ are the degrees of the irreducible factors of \bar{f} (over

$GF(p)$); in fact, if \bar{g} is an irreducible factor of degree d of \bar{f} and α is one of its roots, then the other ones are $\alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}$.

Thus factoring \bar{f} , via lifting ϑ to an element of G gives the cycle lengths of some element of the Galois group.

Cebotarev density theorem guarantees that the set of primes that, through this procedure, yield a fixed element of G has density such that each conjugacy class of elements is equiprobable when a random p is chosen.

So, repeating the above for “many” primes allows one to gather enough information to give an estimate about the distribution of the cycle lengths of the elements of G . Parker’s lemma (see Section 1.2) directly connects them with the Parker vector of G .

To summarise, reducing f modulo p for “many” p ’s gives us the cycle lengths of “many” elements of G , which in turn allows us to give an estimate of the Parker vector of G .

We shall not return to the point of view shown in this section, but for an example of its application, in Section 1.3.

1.2 Definition, first properties and Parker’s Lemma

Let G be a permutation group of degree n . We can identify it with a subgroup of S_n , the symmetric group on n points. Define \mathcal{C}_i to be the set of all the cycles of length i appearing in the elements of G , written as products of disjoint cycles, and define $\mathcal{C} := \bigcup_{i=1}^n \mathcal{C}_i$. Obviously, this set is non-empty

as, for all G , $\mathcal{C}_1 = \{(1), (2), \dots, (n)\}$, these cycles appearing in the identity element.

We can define in a natural way an action of G on the set \mathcal{C} : given $g \in G$ and $(a_1, a_2, \dots, a_k) \in \mathcal{C}$, we set

$$(a_1, a_2, \dots, a_k)^g := (a_1^g, a_2^g, \dots, a_k^g).$$

Equivalently, we can say that the action is defined by conjugation (in S_n , as a single cycle is not in general an element of G).

It is obvious from the definition and from elementary properties of conjugacy in S_n that each orbit of this action must be contained in one of the \mathcal{C}_i 's. Call $p_i(G)$ (or simply p_i , when no possible misunderstanding arises) the number of orbits of this action, which are contained in \mathcal{C}_i ; that is, the number of orbits on i -cycles.

Then the sequence $\mathbf{p}(G) = (p_1(G), p_2(G), \dots, p_n(G))$ is the *Parker vector* of the group G . Sometimes, we will consider $\mathbf{p}(G)$ as an infinite sequence whose entries are eventually zero: $(p_1(G), p_2(G), \dots, p_n(G), 0, 0, \dots)$.

Moreover, it is clear that $p_1(G) = 1$ is equivalent to saying that G is transitive, as the set \mathcal{C}_1 of 1-cycles is (in bijection with) the set of points on which G acts. In general, $p_1(G)$ is equal to the number of orbits of G .

In a few cases, the Parker vector of a group is readily computed: for instance, knowing that two cycles are conjugate in S_n if and only if they have the same length, we can conclude that the Parker vector of S_n is $(1, 1, \dots, 1)$ (n components).

The main result about Parker vectors is the following, due to Richard A. Parker (he gave the definition and some results about the vectors at the 1996 “Groups at St. Andrews” conference, but nothing appears to have been published by him; the definitions and standard results can be found in [Ca98]).

Theorem 1.2.1 (Parker’s lemma) *Let G and \mathcal{C}_i be as above. Let $c_k(g)$ be the number of k -cycles of the element $g \in G$. Then the number of orbits of G on \mathcal{C}_k is*

$$p_k(G) = \frac{1}{|G|} \sum_{g \in G} k c_k(g).$$

Proof Write out a list of all the elements of G in cycle form. There are altogether $n \cdot |G|$ symbols from $\{1, \dots, n\}$ in this list, not counting “(” and “)”. We claim that, for any orbit of G on its k -cycles, the cycles in this orbit cover exactly $|G|$ symbols in the list. It immediately follows that the number of orbits on k -cycles is $1/|G|$ times the number of points in the k -cycles of G .

Let c be a cycle of $g \in G$ of length k . The set of elements of G containing c is a coset Hg , where H is the pointwise stabiliser of c . So the number of such elements is equal to $|H|$.

The stabiliser of c is $H\langle g \rangle$, because it can only rotate the points of c according to some power of g . So the number of distinct cycles obtained from c by the action of G is equal to $|G : H\langle g \rangle|$.

Thus the number of cycles in the orbit occurring in the array (counting repetitions) is $|H| \cdot |G : H\langle g \rangle| = |G|/k$, and so the number of symbols lying

in such cycles is $|G|$. ◇

A straightforward consequence of the fact that $\sum_{k=1}^n kc_k(g) = n$, for each $g \in G$, and of the lemma is its

Corollary 1.2.2 *The number of orbits of G on \mathcal{C} is equal to n .*

Let us remark that, by assuming $k = 1$ in the statement of Parker's Lemma, one gets the so-called Burnside Lemma (or Orbit-Counting Lemma):

$$\text{number of orbits of } G = p_1(G) = \frac{1}{|G|} \sum_{g \in G} c_1(g) = \frac{1}{|G|} \sum_{g \in G} \text{fix}(g),$$

where $\text{fix}(g)$ is the number of points fixed by g , which is equal to the number of 1-cycles in its cycle decomposition.

As it always happens for concepts relative to groups, or group actions, it is interesting:

- 1) to determine them explicitly for particular groups, or families of groups, when possible;
- 2) to understand when and how it is possible to determine them for a group, assuming one already knows them for a related group (subgroup, factor group, product etc.).
- 3) to decide which groups, or classes of groups, are determined by them.

In the remainder of this chapter, and indeed in this whole work, we shall do the first steps in these directions, for what concerns Parker vectors.

As a first, elementary, application of Parker's Lemma, we can compute the Parker vector of a cyclic group of prime order p , C_p (in its natural action

on p points). In such a group the identity has p 1-cycles, whereas any other element has exactly one p -cycle. So we get $p_1(C_p) = 1$, $p_p(C_p) = p - 1$, and $p_k(C_p) = 0$ for other values of k . Thus, in this case, p_k is equal to the number of elements of order k . We shall show later (Section 2.1) that this is the case for all cyclic groups in their regular actions and, more generally, for all regular groups.

Furthermore, this example suffices to show that there are in general no “monotonicity” properties for Parker vectors. That is, one cannot in general say a priori that $p_i > p_{i+1}$ or the other way around, nor that $p_i(H) < p_i(G)$ when $H < G$. In fact, when we compare the action of G on its cycles with that of H on its, we remark that both the set on which the actions are defined and the group acting have increased, so we cannot hope, in general, to get much information about $\mathbf{p}(G)$ from $\mathbf{p}(H)$ or the other way around.

We shall nevertheless find such relations in particular cases, as in the relationship between a transitive permutation group and its point stabiliser.

As another example, let us consider the alternating groups A_n . In these groups, cycles of all lengths less than or equal to $n - 2$ appear. If n is odd, an $(n - 1)$ -cycle (with a 1-cycle) is an odd permutation, so $p_{n-1}(A_n) = 0$ (n odd), while there are at least two conjugacy classes of n -cycles (in S_n , the cycles $(1\ 2\ \dots\ (n-2)\ (n-1)\ n)$ and $(1\ 2\ \dots\ (n-2)\ n\ (n-1))$ are conjugate by an odd permutation). So, $p_n(A_n) = 2$ (n odd), and by Corollary 1.2.2, $p(A_n) = (1, 1, \dots, 1, 0, 2)$ (n odd).

If n is even, an analogous reasoning leads to $p(A_n) = (1, 1, \dots, 1, 2, 0)$ (n

even).

The Parker vectors enjoy some useful “multiplicative” properties with respect to direct and wreath product. We state here the main result, and delay most of its proof until, in chapter 4, the necessary machinery will be developed.

Proposition 1.2.1 *Let G and H be permutation groups, on the sets Ω and Δ respectively. Then*

1. *in the action of $G \times H$ on the disjoint union of Ω and Δ ,*

$$p_k(G \times H) = p_k(G) + p_k(H);$$

furthermore, if K is any subcartesian product of G and H , again

$$p_k(K) = p_k(G) + p_k(H).$$

2. *in the action of $G \times H$ on the cartesian product $\Omega \times \Delta$,*

$$p_k(G \times H) = \sum_{\substack{i,j \\ \text{lcm}(i,j)=k}} p_i(G)p_j(H);$$

3. *in the (imprimitive) action of the wreath product $G \wr H$ on $\Omega \times \Delta$,*

$$p_k(G \wr H) = \sum_{i|k} p_i(G)p_{k/i}(H).$$

Proof The first statement is obvious. For instance, if $g = \gamma_1\gamma_2 \dots \gamma_m \in G$ and $h = \delta_1\delta_2 \dots \delta_n \in H$ (where the γ_i and the δ_j are disjoint cycles), then the pair $(g, h) = \gamma_1 \dots \gamma_m \delta_1 \dots \delta_n$; so $c_k((g, h)) = c_k(g) + c_k(h)$. The other two statements will be proved in section 4.2. ◇

Looking at $\mathbf{p}(G)$ as an infinite sequence whose terms are eventually zero, we can rephrase 1. and 3., respectively, as

$$\mathbf{p}(G \times H) = \mathbf{p}(G) + \mathbf{p}(H)$$

and

$$\mathbf{p}(G \wr H) = \mathbf{p}(G)\mathbf{p}(H).$$

Let us remark that the second operation can be regarded as a convolution product.

This proposition provides examples of pairs of non-isomorphic groups, with the same Parker vectors. In fact, for any G and H , it implies that $p_k(G \wr H) = p_k(H \wr G)$ (whereas, of course, in general $G \wr H$ is not isomorphic to $H \wr G$). Also, 1. shows that all subcartesian products of G and H have the same Parker vector. Further, if $|G|$ and $|H|$ are coprime, 2. and 3. show that $p_k(G \wr H) = p_k(G \times H)$, so that, in general, we cannot distinguish abelian groups by their Parker vectors: consider for instance $C_2 \times C_3$ and $C_2 \wr C_3$. This also gives an example of groups with the same Parker vector but different orders.

The importance of statement 1. about the subcartesian products lies in that it gives us the complete knowledge of the Parker vectors of the intransitive groups when we know the Parker vectors of their transitive constituents.

So, in what follows, unless otherwise stated, we can always assume the groups we work with to be transitive.

Unfortunately, nothing similar seems to hold for the somehow analogous

“reduction” of imprimitive groups obtained by considering them as subgroups of a wreath product. The problem, of course, stems from the nonexistence of a unique decomposition into something like “primitive components”. For instance, if we consider S_3 in its regular action on itself, it has Parker vector $(1, 3, 2, 0, 0, 0)$. The two possible choices for a block of imprimitivity, the subgroup of order 3 and a subgroup of order 2, give embeddings of S_3 respectively into $C_3 \wr C_2$, with Parker vector $(1, 1, 2, 0, 0, 2)$, and into $C_2 \wr D_3$, whose Parker vector is $(1, 2, 1, 1, 0, 1)$.

We have already remarked, or it is obvious, that in the Parker vector of a permutation group one can directly read its degree and the number of its orbits. Moreover, the Parker vector determines the exponent of the group (that is, the minimum non-negative integer n such that, for all g in G , $g^n = 1$); indeed, $\exp(G) = \text{lcm}\{k : p_k(G) \neq 0\}$.

Let us conclude this section with an example of how Prop. 1.2.1 can be applied. We shall determine the Parker vector of the Sylow p -subgroups of S_n , their structure being a direct product of wreath products of cyclic groups of prime order. More precisely (see for instance [DM96]), to construct a Sylow p -subgroup P of S_n , write n in base p : $n = n_0 + n_1p + n_2p^2 + \dots + n_r p^r$. Next, recursively define $P_0 := \{1\}$, $P_1 := C_p$, and $P_m := P_{m-1} \wr C_p$ in its imprimitive action. Then, P is isomorphic to the direct product of $P_0 \times \dots \times P_0$ (n_0 times) times $P_1 \times \dots \times P_1$ (n_1 times) times \dots times $P_r \times \dots \times P_r$ (n_r times).

Thus, by applying the results of this section, we get $p_k(P_m) = \binom{m}{i} (p-1)^i$ if $k = p^i$, and 0 otherwise. In fact, when $m = 1$, this is equivalent to what

has been said for cyclic groups of prime order; for $m > i$, an induction, using the third part of Prop. 1.2.1, gives the result:

$$\begin{aligned}
p_k(P_m) &= p_k(P_{m-1} \wr C_p) = \sum_{l|k} p_l(P_{m-1})p_{k/l}(C_p) \\
&= \sum_{j=0}^i p_{p^j}(P_m)p_{p^{i-j}}(C_p) = p_{p^i}(P_m)p_1(C_p) + p_{p^{i-1}}(P_m)p_p(C_p) \\
&= \binom{m-1}{i} (p-1)^i \cdot 1 + \binom{m-1}{i-1} (p-1)^{i-1} \cdot (p-1) \\
&= (p-1)^i \left(\binom{m-1}{i} + \binom{m-1}{i-1} \right) = \binom{m}{i} (p-1)^i.
\end{aligned}$$

Next, as $P = \prod_{j=0}^r P_j^{n_j}$, adding up the Parker vectors for the P_j 's yields

$$p_k(P) = \begin{cases} \sum_{j=0}^r n_j \binom{j}{i} (p-1)^i & k = p^i \\ 0 & \text{else} \end{cases}. \quad (1.1)$$

For instance, consider S_{30} . We can write its degree as $30 = 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 = 1 \cdot 3 + 1 \cdot 3^3 = 1 \cdot 5 + 1 \cdot 5^2 = 2 \cdot 7^0 + 4 \cdot 7$, and for all the remaining primes (11 to 29) the greater appearing power is the first one. Calling P_p a Sylow p -subgroup of S_{30} and applying (1.1), we get

$$\begin{aligned}
\mathbf{p}(P_2) &= (4, 10, 0, 10, 0, 0, 0, 5, 0, \dots, 0, 1, 0, \dots) \\
\mathbf{p}(P_3) &= (2, 0, 8, 0, 0, 0, 0, 0, 12, 0, \dots, 0, 8, 0, 0, 0) \\
\mathbf{p}(P_5) &= (2, 0, 0, 0, 12, 0, \dots, 0, 16, 0, \dots).
\end{aligned}$$

(where the last non-zero terms are in 16th, 27th, and 25th position respectively). It is always true, by (1.1), that $p_1(= p_{p^0})$ is just the sum of the coefficients of the prime powers.

For the remaining primes, just two components of the Parker vector being different from zero, it suffices to give the first one (the other one, P_p , is 30

minus it): $p_1(P_7) = 6$, $p_1(P_{11}) = 10$, $p_1(P_{13}) = 6$, $p_1(P_{17}) = 14$, $p_1(P_{19}) = 12$, $p_1(P_{23}) = 8$, and $p_1(P_{29}) = 2$.

1.3 Parker vectors and multiple transitivity

The following propositions give useful sufficient conditions on the Parker vector of a group G , for G is transitive or multiply-transitive. So, in particular, we shall be able to identify symmetric and alternating groups (with a single exception) from their Parker vectors.

First of all, the existence of a cycle of length equal to the degree of the group guarantees the group to be transitive: the group contains a cyclic subgroup acting transitively. Therefore:

Proposition 1.3.1 *If G is a permutation group of degree n and $p_n(G) > 0$, then G is transitive.*

Similarly:

Proposition 1.3.2 *If G is as in the previous proposition, and both $p_n(G)$ and $p_{n-1}(G)$ are greater than 0, then G is 2-transitive.*

Proof G is transitive. Further, an element containing an $(n - 1)$ -cycle and its powers fix a point and are transitive on the other ones. \diamond

Proposition 1.3.3 *If G is as before, and all of $p_n(G)$, $p_{n-1}(G)$, $p_{n-2}(G)$, and $p_{n-3}(G)$ are greater than 0, then G is 3-transitive.*

Proof By the previous proposition, G is 2-transitive. Assume from now on that it is not 3-transitive. Then $G_{\alpha\beta}$ has two orbits of size $(n-2)/2$. In fact, we know that there exists an $(n-2)$ -cycle; if it occurred in an element fixing the remaining two points (say, α and β), then $G_{\alpha\beta}$ would be transitive on $\{1, \dots, n\} \setminus \{\alpha, \beta\}$, and the group would be 3-transitive. Therefore, any $(n-2)$ -cycle must occur together with a 2-cycle; so the square of such an element must have cycle structure $((n-2)/2, (n-2)/2, 1, 1)$.

On the other hand, an $(n-3)$ -cycle can occur in an element h of the forms $(n-3, 1, 1, 1)$, $(n-3, 2, 1)$ or $(n-3, 3)$.

In the first case, $G_{\alpha\beta}$ has a (third) orbit of size 1. So, $\frac{n-2}{2} = 1$, and $n = 4$, but the unique group of degree 4 satisfying the hypotheses is S_4 . The second case reduces to first one, by replacing h by h^2 (because $n-3$ is odd, as $(n-2)/2$ is integer).

The third case reduces to the first one if 3 does not divide $n-3$. Otherwise, $3|n-3$, and the third power of an element of the form $(n-3, 3)$ has form $(\frac{n-3}{3}, \frac{n-3}{3}, \frac{n-3}{3}, 1, 1, 1)$. Hence $(n-3)/3 + 1 = (n-2)/2$, and $n = 6$. But the unique groups of degree 6 in which both 5- and 6-cycles occur are $PGL(2, 5)$ and S_6 , which are 3-transitive. \diamond

The occurrence of $PGL(2, 5)$ in the previous argument is significant. In fact, as the next theorem shows, when we ask for all p_k 's ($k = 1, \dots, \deg(G)$) to be greater than 0, that is for cycles of all lengths to occur, we have the strictest bound on possible groups, and the only "exceptional" one is $PGL(2, 5)$.

First, observe that this is equivalent to asking that, for all k , $p_k(G) = 1$, as the components of the Parker vector add up to $\deg(G)$.

Theorem 1.3.1 *If G is a permutation group of degree n , and $p_1(G) = p_2(G) = \dots = p_n(G) = 1$, then, if $n \neq 6$, $G \cong S_n$ in its natural action. When $n = 6$, G is isomorphic to either S_6 or $PGL(2, 5)$ (in its action on 6 symbols, as given for instance by the presentation $\langle (12345), (16)(23)(45) \rangle$).*

Proof By the previous proposition, G is 2-transitive. In particular, it is primitive.

On the other hand, for each natural number $m > 3$, by Bertrand's postulate there exists a prime number p such that $m < p < 2m - 2$. So, for $n > 6$, there exists in G an element with a p -cycle and at least three fixed points. In fact, consider an element g containing a p -cycle; the number of points not comprised in the cycle must be less than p (and at least three) so that, independently of the remaining cycle structure of g , a multiple of g exists such that all these points are fixed.

It is known (Jordan (1873), for instance in [Wi64]) that a primitive group in which such an element occurs must be either A_n or S_n . We have already seen that $p_n(A_n)$ and $p_{n-1}(A_n)$ are different from 1.

So just the case $n \leq 6$ remains, where there is a unique non-symmetric group satisfying the hypotheses, $PGL(2, 5)$. That this is indeed the case, is shown by recalling the general fact that, for any p , $PGL(2, p)$ contains cycles of length $p - 1$, p , and $p + 1$. ◇

Alternating groups too are uniquely determined by their Parker vectors.

Theorem 1.3.2 *If G is a permutation group of odd degree n , and $p_1(G) = p_2(G) = \dots = p_{n-2}(G) = 1$, $p_{n-1}(G) = 0$, $p_n = 2$, then $G \cong A_n$; the same holds if n is even and the requested values for p_{n-1} and p_n are reversed.*

Proof In the even case, one simply observes that $p_1 = 1$ and $p_{n-1}(G) = 2$ guarantees that G is 2-transitive, so we can repeat the argument of the previous theorem.

In the odd case, we know that an $(n - 2)$ -cycle occurs in some element. It has cycle structure either $(n - 2, 2)$ or $(n - 2, 1, 1)$, but in the first case its square must have the second form. Therefore, the subgroup generated by this element is transitive on $n - 2$ points; so either G_α fixes two points and has an orbit of size $n - 2$, or it fixes just one point, and is transitive on the others. The first case would imply that G_α has a block of imprimitivity of size 2, so $2 \mid n$, but n is odd. So the second case holds, G is 2-transitive, and the argument for the symmetric case can be repeated. \diamond

As an example of the application of what we have seen up to now about Parker vectors, let us return to the procedure described in section 1.1, putting it into practice on the polynomial $f = x^5 - x - 1$ over \mathbf{Z} (in a somewhat different context, this example comes from [La93]). Reducing mod 5 shows that this polynomial is irreducible. Reducing mod 2 gives the irreducible factors $(x^2 + x + 1)$ and $(x^3 + x^2 + 1)$. Reducing mod 23 gives the factorisation $\bar{f} = (x + 9)(x^4 + 14x^3 + 12x^2 + 7x + 5)$. So we have elements with cycle

structure, respectively, (5), (3, 2), and (4, 1); thus they give contributions greater than zero to all the components of the Parker vector of the Galois group G of f . Therefore, $p(G) = (1, 1, 1, 1, 1)$ and, by Theorem 1.3.1, $G \cong S_5$. (Of course, in this particular case, as an element of the form (3, 2) entails one of the form (2, 1, 1, 1), its third power, the group could more directly be identified by the presence of a 5-cycle and a transposition.)

1.4 A possible generalisation

A definition can be given of a vector $\mathbf{p}(\chi)$ for χ a character of a finite group G . If π is a permutation character, then $\mathbf{p}(\pi)$ actually is the Parker vector of (the corresponding permutation representation of) G .

Let χ be a character of the finite group G . Define

$$s_k(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g^k)$$

and

$$p_k(\chi) := \sum_{i|k} \mu(k/i) s_i(\chi),$$

where μ is the Möbius function. The sequence $\mathbf{p}(\chi) = (p_1(\chi), \dots, p_k(\chi), \dots)$ is a *generalised Parker vector* of G with respect to the character χ .

A fundamental property of a generalised Parker vector is

Lemma 1.4.1 $p_k(\chi) = 0$ when $k \nmid |G|$.

Proof Indeed, consider the map of G into itself (in general not a homomorphism) $\varphi_k : g \mapsto g^k$. When $(k, |G|) = 1$, there exist a, b such that

$ak + b|G| = 1$, so that, for all $g \in G$, $g = g^{ak+b|G|} = g^{ak}g^{b|G|} = g^{ak}$. So there is an element (g^a) the k -th power of which is equal to g . This means that, when $(k, |G|) = 1$, φ_k is surjective.

Reasoning in the same way, we see that if $(k, |G|) = d$, then $\varphi_k(G) = \varphi_d(G)$. Further, if $\{1, g_1, g_2, \dots\}$ is the set of the elements of G , consider the $|G|$ -tuples $(\varphi_k(1), \varphi_k(g_1), \varphi_k(g_2), \dots)$ and $(\varphi_d(1), \varphi_d(g_1), \varphi_d(g_2), \dots)$: they are equal up to ordering.

A consequence of this is the fact that

$$s_k(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^k) = s_{(k, |G|)}(\chi). \quad (1.2)$$

Next, fix a k not dividing $|G|$. Choose p such that p^m is the greatest power of p dividing $|G|$, whereas p^{m+1} divides k for some m , possibly 0. As in the definition a generalised Parker vector each summand is multiplied by $\mu(k/i)$, we can consider just the i 's such that k/i is squarefree.

If $p \nmid k/i$, then both i and i/p are divisors of k and both k/i and $k/(i/p)$ are squarefree. So $\mu(k/i) = -\mu(k/(i/p))$. On the other hand, $(|G|, i) = (|G|, i/p)$ because k/i being squarefree implies i contains the whole power of p dividing $|G|$; so, by (1.2), $s_i = s_{i/p}$ and the corresponding terms cancel out in the expression for p_k .

An analogous argument holds when $p|k/i$, by looking at the divisors i and ip of k (here $(|G|, i) = (|G|, ip)$). \diamond

From this lemma, an important property of the generalised Parker vectors follows, which, as the lemma itself, extends the corresponding property of the

standard Parker vectors.

Proposition 1.4.1 *If χ is a character of the finite group G and $\mathbf{p}(\chi) = (p_k(\chi))$ is the generalised Parker vector of G with respect to χ , then just finitely many components of $\mathbf{p}(\chi)$ are non-zero, and*

$$\sum_i p_i(\chi) = \chi(1).$$

Proof The first claim is a trivial consequence of the lemma. For the second, simply invert the definition of p_k by Möbius inversion formula, which yields $s_k = \sum_{i|k} p_i$. So (setting $n = |G|$):

$$\sum_i p_i = \sum_{i|n} p_i = s_n = \frac{1}{|G|} \sum_{g \in G} \chi(g^n) = \frac{1}{|G|} \sum_{g \in G} \chi(1) = \chi(1).$$

◇

Parker's lemma is equivalent to saying that if π is a permutation character, then $\mathbf{p}(\pi)$ actually is the Parker vector of the corresponding permutation representation of G . In fact, keeping in mind that the value of π on an element g is $\text{fix}(g)$, the number of its fixed points, and that $\pi(g^k) = \text{fix}(g^k) = \sum_{i|k} i c_i(g)$,

$$\begin{aligned} p_k(\pi) &= \sum_{i|k} \mu\left(\frac{k}{i}\right) s_i(\pi) = \frac{1}{|G|} \sum_{i|k} \mu\left(\frac{k}{i}\right) \sum_g \pi(g^i) \\ &= \frac{1}{|G|} \sum_g \sum_{i|k} \mu\left(\frac{k}{i}\right) \sum_{j|i} j c_j(g) = \frac{1}{|G|} \sum_g k c_k(G) = p_k(G). \end{aligned}$$

This guarantees that if we take a character χ and find a component of the corresponding Parker vector which is not a natural number, then χ is not a permutation character. This gives a further condition to detect “permutation

character candidates”, which adds to the standard ones: $\chi(g)$ must be a nonnegative integer for all g in G , $\chi(1)$ must divide $|G|$ etc.

The numbers $s_k(\chi)$ have another interpretation: the linear combination of the irreducible characters of G with the $s_k(\chi)$ as coefficients is an integer-valued class function $\vartheta_k = \sum_{\chi \in \text{Irr}(G)} s_k(\chi)\chi$ which associates with each conjugacy class of G the number of “ k -th roots” its elements have in G . In more precise terms, $\vartheta_k(g) = |\{h \in G : h^k = g\}|$. It can be shown that, given an irreducible character χ , the class function $\chi^{(n)} : g \mapsto \chi(g^n)$, for a fixed n , is a generalised (or virtual) character, i.e. a difference of characters. So, $s_k(\chi) = [\chi^{(k)}, 1_G]$, for $\chi \in \text{Irr}(G)$, is an integer. In particular, $s_1(\chi)$ is the multiplicity of 1_G in χ .

Moreover, by the Frobenius-Schur theorem, $s_2(\chi)$ is equal to the Frobenius-Schur index ϵ_χ , which is by definition equal to 1 if χ is a character afforded by a real representation; to -1 when χ is real-valued but not afforded by any real representation; and to 0 when χ is not real-valued.

The fact that the character of a permutation representation determines the Parker vector of (that representation of) a group tells us that in general the Parker vector of a group does not tell whether that group is primitive or not. Indeed, in [GS92], Guralnick and Saxl show an example of a group G with two subgroups H, K such that $(1_H)^G = (1_K)^G$ but H is maximal whereas K is not. This gives two permutation representations of G , respectively on the cosets of H and K , with the same permutation character but one of which is primitive whereas the other one is not. This implies that there

are two groups, one primitive and the other imprimitive, the two permutation groups induced by G , with the same Parker vector.

Let us see an example of a generalised Parker vector. If we consider the irreducible character $\chi = \pi - 1$ of S_4 , where π is the standard permutation representation, that is the character which takes values $(3, 1, 0, -1, -1)$ on the classes $(1^4, 1^2 2, 3, 2^2, 4)$, respectively, the definitions give the following values for the s_k 's and the p_k 's:

| | | | | | | | | | | | | | |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|-----|
| k | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ... |
| s_k | 0 | 1 | 1 | 2 | 0 | 2 | 0 | 2 | 1 | 1 | 0 | 3 | ... |
| p_k | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |

As it should be, the sum of the p_k 's is equal to 3, the dimension of the character.

For the character-theoretic results quoted in this section see for instance [Is76]; for the connections with Parker vectors, see [Ca98].

Chapter 2

Parker vectors of regular and Frobenius groups

2.1 Regular groups

We recall the definition.

Definition A permutation group G is called *semiregular* if the unique element of G that fixes some point is the identity (in other words every stabiliser is trivial). A transitive semiregular group is called *regular*.

Up to action equivalence, all the examples of regular groups are given by any group acting on itself by right multiplication. Regular and semiregular groups enjoy several properties that make them especially easy to work with and, at the same time, not very interesting.

Proposition 2.1.1 *A permutation group G is semiregular if, and only if, any element g of G is a product of disjoint cycles of the same length.*

Proposition 2.1.2 *A permutation group G is regular if, and only if, it is transitive and its degree is equal to its order.*

Proposition 2.1.3 *If a cycle appears in two elements g and g' of a regular permutation group, then $g = g'$.*

The following property of the cycles of the elements of a regular group is useful in view of studying the Parker vector of such a group.

Proposition 2.1.4 *Let γ be a cycle of an element g of a regular permutation group G , $h \in G$. Then:*

$$\gamma^h \text{ is a cycle of } g \Leftrightarrow h \in C_G(g).$$

Proof Both implications follow from the fact that if γ^h is also an element of g^h , then, by 2.1.3, $g^h = g$. ◇

Corollary 2.1.1 *With G as above, given an element g in G , the number of orbits on cycles, represented in g (that is, the number of non-conjugate cycles appearing in g) is $|G|/|C_G(g)|$, that is the cardinality of the conjugacy class of g .*

Proof As G is regular, the number of cycles of g is $|G|/|\langle g \rangle|$. Also, the number of cycles of g in the same orbit as γ is equal to the size of an orbit on cycles of g of $C_G(g)$ (so that it is meaningful to say something about “orbits on cycles of g ”).

So the number of orbits represented in g is $\frac{|G|}{|\langle g \rangle|} / \frac{|C_G(g)|}{|\langle g \rangle|}$, as it was to be shown. ◇

Corollary 2.1.2 *Again with G as above, $p_m(G)$ is equal to the number of elements of order m in G .*

Proof Every conjugacy class of elements of order m contributes its own cardinality to p_m , by Cor. 2.1.1. \diamond

The previous results give some necessary conditions for a group with given Parker vector to be regular (for instance, the component p_i can be non-zero only if i divides the degree of the group).

Unfortunately, one cannot hope to determine the regularity of a group just by looking at its Parker vector. For instance, as it was already pointed out, $C_2 \times C_3$ in its regular action and $C_2 \wr C_3$ have the same Parker vector.

In particular, we now know the Parker vector for the cyclic groups in their standard (that is regular) action. For them, the last corollary amounts to the following proposition.

Proposition 2.1.5 *If $d|n$, then $p_d(C_n) = \varphi(d)$; otherwise, it is equal to 0.*

Proof In fact, $\varphi(d)$ is just the number of elements of order d in the group, if any. \diamond

Knowing the Parker vectors of the cyclic groups, we can derive the Parker vectors of the dihedral groups. If we denote the dihedral group of order $2n$ by D_n and if n is $2k$ or $2k+1$ (k integer), a moment's thought will show that

$$\begin{aligned} p_1(D_n) &= 1 \\ p_2(D_n) &= k \end{aligned}$$

$$p_i(D_n) = \begin{cases} 0 & i \nmid n \\ \varphi(i)/2 & i \mid n \end{cases} \quad (\text{for } i > 2).$$

In particular, when n is odd, D_n is a Frobenius group, and this expression is a particular case of the more general one shown in section 2.3.

2.2 Relationship between the Parker vector of G and the Parker vector of G_α

Consider a transitive permutation group G , so that it makes sense to uniquely talk about its stabiliser G_α . Then it is in general possible to say something about the relationship between the Parker vector of G and the Parker vector of G_α . In some more particular cases, what follows will convey more information.

Proposition 2.2.1 *Let S be the set of the derangements (fixed point free elements) of G , a transitive permutation group of degree n . Then, for $k > 1$:*

$$p_k(G) \leq p_k(G_\alpha) + \frac{1}{|G|} \sum_{g \in S} kc_k(g).$$

Equality holds if and only if each element containing a k -cycle fixes at most one point.

Proof It is just an immediate consequence of Parker's Lemma:

$$\begin{aligned} p_k(G) &= \frac{1}{|G|} \sum_{g \in G} kc_k(g) \\ &\leq \frac{1}{|G|} \left(kc_k(1) + \sum_{\alpha \in \Omega} \sum_{\substack{g \in G_\alpha \\ g \neq 1}} kc_k(g) + \sum_{g \in S} kc_k(g) \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{|G|} \left(n|G_\alpha|p_k(G_\alpha) + \sum_{g \in S} kc_k(g) \right) \\
&= p_k(G_\alpha) + \frac{1}{|G|} \sum_{g \in S} kc_k(g)
\end{aligned}$$

The claimed condition for equality to hold is equivalent to saying that, for $\alpha \neq \beta$, elements in $G_\alpha \cap G_\beta$ have no k -cycles, so that summing over all the non-identity elements that fix at least one point is the same as summing over all the elements in G_α when α varies in Ω . \diamond

From this a characterisation follows for the corresponding components of $p(G)$ and $p(G_\alpha)$ to be equal.

Proposition 2.2.2 *For G as above, $p_k(G) = p_k(G_\alpha)$ if and only if each element containing a k -cycle fixes exactly one point.*

As examples of situations in which the hypothesis of this proposition is satisfied, consider Frobenius groups (see next section) or Zassenhaus groups. Let us recall that a *Zassenhaus group* is a 2-transitive group G in which, for any distinct α, β, γ , $G_{\alpha\beta\gamma} = \{1\}$ (one usually adds the condition that G has no regular normal subgroup, to exclude Frobenius groups and a known class of groups of semilinear mappings; see [HB82], chap. XI); they are completely classified as either particular semilinear projective groups or the Suzuki groups $Sz(2^{2n+1})$ for $n = 1, 2, \dots$ (again, see [HB82]). In a Zassenhaus group G , for $k|n-1$, an element with a k -cycle is in a stabiliser G_α (because $k|n-1$ implies $k \nmid n$), and it is a derangement on $\Omega \setminus \{\alpha\}$ (otherwise $k|n-2$). So, $p_k(G) = p_k(G_\alpha)$, with G_α a Frobenius group (see next section).

A straightforward, very useful consequence of the previous proposition is:

Corollary 2.2.1 *If G is a transitive permutation group of degree n , $p_{n-1}(G) = p_{n-1}(G_\alpha)$.*

2.3 Frobenius groups

Again, we begin by recalling the definition.

Definition A *Frobenius group* is a transitive non regular permutation group G such that, for all $g \in G \setminus \{1\}$, g has at most one fixed point.

The main result about finite Frobenius groups is the following (see for instance [Pa68]).

Theorem 2.3.1 (Structure theorem for finite Frobenius groups) *Let G be a finite Frobenius group, and let K be the subset of all its elements with no fixed points, plus the identity. Then*

1. K is a subgroup of G (so, it is a normal regular subgroup);
2. for all primes $p \neq 2$, the Sylow p -subgroups of G_α are cyclic; the Sylow 2-subgroups are cyclic or generalised quaternion;
3. if G_α is not soluble, it has exactly one non-abelian composition factor, and this is isomorphic to A_5 ;
4. K is nilpotent.

We shall mainly use the first of these facts, in conjunction with the obvious implications that $G = G_\alpha K$ and $G_\alpha \cap K = \{1\}$, so that each element of G either lies in a subgroup conjugate to G_α (that is, some G_β) or in K . In the usual terminology, K is the *Frobenius kernel* and any G_α is a *Frobenius complement*.

Furthermore, one can easily see that the fact that the set K is indeed a non trivial subgroup characterises Frobenius (or regular) groups; the same holds for its cardinality being equal to the degree of the group.

The first fact is a consequence of a theorem by Zantema ([Za82]): the subgroup generated by the derangements is transitive and contains every element whose number of fixed points is different from 1. In our case, this means that all elements not in K (that, being a subgroup, is the same as $\langle K \rangle$) fix exactly one point, so the group is Frobenius (or regular).

The second fact (that is, $|K| = \text{deg}(G)$ implies G Frobenius) is shown by a direct counting argument. Call x_i the number of elements of G that fix exactly i points. So, $\sum x_i = |G|$ (trivial) and $\sum ix_i = |G|$ (“Burnside’s Lemma”); subtracting yields $\sum(i-1)x_i = 0$, or $x_0 = x_2 + 2x_3 + \dots + (n-1)x_n$. As the identity is the unique element fixing n points, $x_n = 1$. So, in general $x_0 \geq n - 1$; the equality holds if and only if $x_2 = \dots = x_{n-1} = 0$, that is if the group is Frobenius (or regular).

By applying the results in the previous section, we can give a complete description of a Frobenius group Parker vector when we know the Parker vectors of its kernel and its complement.

Proposition 2.3.1 *Let G be a Frobenius group of degree m , acting on Ω . If the Parker vector of G_α is $\mathbf{p} = (p_1, p_2, \dots, p_{m-1})$, and the Parker vector of the Frobenius kernel K is \mathbf{p}' , then the Parker vector of G is $\mathbf{p}'' := \mathbf{p} + \mathbf{p}'/|G_\alpha|$, but with the first component changed to 1.*

Proof We apply Proposition 2.2.1 to the present situation. Here all the elements of G fix at most one point, so equality holds for each $k > 1$. Furthermore, now $S \cup \{1\}$ is the subgroup K . So, the last summand, $\frac{1}{|G|} \sum_{g \in S} kc_k(g)$, becomes

$$\frac{|K|}{|G|} \frac{1}{|K|} \sum_{g \in K} kc_k(g) = \frac{1}{|G_\alpha|} p'_k.$$

For $k = 1$, of course, $p'_1 = 1$, because G is transitive. \diamond

It may be useful to emphasise the fact that in the sum appearing in the previous proposition, for each k , at most one of p_k and p'_k is different from 0. Indeed, this follows from the general fact that for any finite group G , if i does not divide $|G|$, then the corresponding component p_i of the Parker vector is 0. Here, $|K| = m$, $|G_\alpha|$ divides $m - 1$ because G_α is semiregular on $\Omega \setminus \{\alpha\}$ and each element in G is either in K or in a conjugate of G_α .

The expression for $\mathbf{p}(D_n)$ (n odd) given at the end of section 2.1 can now be interpreted as being obtained from

$$\mathbf{p} = \mathbf{p}(G_\alpha) = \mathbf{p} \left(\left\langle (2 \ n)(3 \ n-1) \dots \left(\frac{n+1}{2} \ \frac{n+1}{2} + 1 \right) \right\rangle \right) = \left(\frac{n-1}{2}, \frac{n-1}{2} \right)$$

and

$$\mathbf{p}' = \mathbf{p}(K) = \mathbf{p}(C_n)$$

by applying the proposition above.

There is a partial converse of the previous proposition, giving a sufficient condition for a group to be Frobenius, looking at its and its stabiliser's Parker vectors.

Proposition 2.3.2 *If G is a transitive group and $p_k(G) = p_k(G_\alpha)$ for all k such that $k \mid |G_\alpha|$ and $k \neq 1$, then G is a regular or Frobenius group.*

Proof Each element of G_α must include a k -cycle for one of the aforementioned k 's. So, by prop. 2.2.2, under the given hypothesis, each element of G_α fixes exactly one point, that is, no other point but α . \diamond

Another partial converse of Prop. 2.3.1, giving this time a necessary condition, but not requesting any knowledge about the stabiliser of the group, is the following

Proposition 2.3.3 *A necessary condition for a transitive group G of degree n to be Frobenius is that the following hold:*

- $p_k(G) = 0$ unless either $k \mid n$ or $k \mid n - 1$;
- $r := n - 1 - \sum_{\substack{k \mid n-1 \\ k \neq 1}} p_k(G)$ divides $n - 1$;
- $\frac{n-1}{r} \sum_{\substack{k \mid n \\ k \neq 1}} p_k(G) + 1 = n$.

Proof The first condition is implied by the already mentioned facts that $|K| = n$, $|G_\alpha|$ divides $n - 1$, and $G = K \cup \cup_\alpha G_\alpha$.

By Prop. 2.3.1 (or Prop. 2.2.2), if $k|n-1$ and $k \neq 1$, then $p_k(G) = p_k(G_\alpha)$.

The degree of G_α is $n-1$; so, by Parker's lemma, the number of orbits of G_α plus $\sum_{\substack{k|n-1 \\ k \neq 1}} p_k(G)$ is equal to $n-1$. Hence r , as defined above, is the number of orbits of G_α and must divide $n-1$ by the semiregularity of G_α . This gives the second condition.

To get the third one, divide $n-1$ by r to get the cardinality of each orbit of G_α , which is equal to the order of G_α , again by its semiregularity; next, applying Parker's lemma yields the relation. \diamond

Let us explicitly remark that, assuming that we know the Parker vector of a Frobenius group, we immediately know the Parker vectors of its Frobenius kernel and of its stabiliser G_α , given respectively by

$$p_k(K) = \begin{cases} 1 & k = 1 \\ \frac{n-1}{r} p_k(G) & k \neq 1, k|n \\ 0 & k \nmid n \end{cases}$$

and

$$p_k(G_\alpha) = \begin{cases} r & k = 1 \\ p_k(G) & k \neq 1, k|n-1 \\ 0 & k \nmid n-1 \end{cases},$$

where r is defined as above.

Let us conclude this section by explicitly working out the calculation of the Parker vector of $G = Sz(8)$, the Suzuki group of order $2^6 \cdot 5 \cdot 7 \cdot 13$ and degree 65. It is a Zassenhaus group; its stabiliser G_α is a Frobenius group that has in the kernel K seven involutions and 56 elements of order 4, while the complement $G_{\alpha\beta}$ of K is cyclic of order 7. So, by proposition 2.3.1, $p_1(G_\alpha) = p_2(G_\alpha) = 1$, $p_4(G_\alpha) = 8$, and $p_7(G_\alpha) = 54$.

Consequently, $p_1(G) = 1$ and, by prop. 2.2.2 and the remarks after it, $p_2(G) = 1$ and $p_4(G) = 8$. By other considerations we can complete the Parker vector of $Sz(8)$.

Let $I_i = \{g \in Sz(8) : \text{fix}(g) = i\}$, for $i = 0, 1, 2$; thus, $G = \{1\} \cup I_0 \cup I_1 \cup I_2$.

We can compute the cardinality of the I_i 's:

$$\begin{aligned} |I_1| &= 65|K \setminus \{1\}| = 65 \cdot 63; \\ |I_2| &= \binom{65}{2} |G_{\alpha\beta}\{1\}| = 65 \cdot 64 \cdot 3; \\ |I_3| &= |G| - |I_1| - |I_2| - 1. \end{aligned}$$

Using for the Parker vector the expression, equivalent to the one given by Parker's lemma,

$$p_k(G) = \frac{1}{|G|} \sum_{i|k} \mu\left(\frac{k}{i}\right) \sum_{g \in G} \text{fix}(g^i)$$

(see remarks after Prop. 1.4.1), we get $p_{13}(G) = (1/|G|) \sum_g \text{fix}(g^{13}) - 1$. The elements in I_1 and in I_2 have orders coprime with 13, so for them $\text{fix}(g^{13}) = \text{fix}(g)$. The number of elements of order 13 is $12n_{13}$, where n_{13} is the number of Sylow 13-subgroups. Of course, each element containing a 13-cycle has order 13, otherwise its 13-th power would fix more than two elements and be different from the identity. Hence:

$$\begin{aligned} p_{13}(G) &= \frac{1}{G}(65(1 + 12n_{13}) + |I_1| + 2|I_2|) - 1 \\ &= \frac{65 + 65 \cdot 12n_{13} + 65 \cdot 63 + 65 \cdot 64 \cdot 6}{65 \cdot 64 \cdot 7} - 1 = \frac{3n_{13}}{112}. \end{aligned}$$

Now, by Sylow's theorem, $n_{13} \equiv 1 \pmod{13}$ and $n_{13} \mid 2^6 \cdot 5 \cdot 7$; further, we know that $112 = 2^4 \cdot 7 \mid n_{13}$. Thus $n_{13} \in \{112, 224, 448, 560, 1120, 2240\}$ and

checking the possible values, one finds that only $560 \equiv 1 \pmod{13}$. Therefore, $p_{13}(G) = 15$. By a similar argument, $p_7(G)$ is shown to be equal to 27; finally, $p_5(G) = 65 - (p_1 + p_2 + p_4 + p_7 + p_{13}) = 13$.

Summarising, $\mathbf{p}(Sz(8)) = (1, 1, 0, 8, 13, 0, 27, 0, 0, 0, 0, 0, 15, 0, \dots, 0)$.

Chapter 3

Permutation groups with a regular normal subgroup and their Parker vectors

The Frobenius groups are a particular case of the more general situation of a permutation group which has a normal subgroup acting regularly. This fact is often sufficient to understand something about the group, keeping some of the results which hold for Frobenius groups.

3.1 Permutation groups with a regular subgroup

The even more general situation of a permutation group with a regular subgroup, not necessarily normal, is radically less manageable.

First of all, if G has a regular subgroup, it is of course transitive. Then, in common with the “normal” case, if G has a regular subgroup R , then $G = G_\alpha R = R G_\alpha$ and $R \cap G_\alpha = \{1\}$.

But the main difference when R is not normal lies in the fact that in this

case G is not contained in the holomorph of R . We recall that the *holomorph* $\text{Hol}(R)$ of a regular group R of degree n is its normaliser in S_n ; it can be shown it is isomorphic to $R : \text{Aut}(R)$ (for instance, in [Ro78], Chap.9).

So, in a sense, when $G \not\leq \text{Hol}(R)$ one has a far less strong relation between R and the whole group. For instance, we cannot hope to get results such as Prop. 2.3.1, nor the standard result about regular normal subgroups (see for instance [Wi64]):

Theorem 3.1.1 *Let r be a normal regular subgroup of G . Then the permutation actions of G_α on $\Omega \setminus \{\alpha\}$ and of G on $R \setminus \{1\}$ by conjugation are equivalent.*

3.2 The case of the normal regular subgroup

On the contrary, in the case in which the regular subgroup is normal we can generalise some of the properties of the Frobenius groups.

For instance, we can prove a result similar to the following.

Theorem 3.2.1 *The Frobenius kernel of a primitive Frobenius group is elementary abelian.*

In the new context, we can prove an analogous result, forfeiting the Frobenius condition, and adding a request about the orders of the “kernel” and its complement.

Proposition 3.2.1 *Let G be a primitive permutation group acting on Ω . Let*

K be a normal regular subgroup of G , $(|K|, |G_\alpha|) = 1$. Then K is elementary abelian.

Proof Since G is primitive, G_α is maximal for each α . So K is a minimal normal subgroup (if $H < K$, H normal, then $G_\alpha < HG_\alpha < G$ with proper inclusions). Therefore, K is characteristically simple (that is, it has no non-trivial characteristic subgroups); by the structure theorem for characteristically simple groups, $K = S \times S \times \dots \times S$, with S simple.

So, it suffices to show that K has to be a p -group for some prime p , as the only simple p -groups are the cyclic ones.

Now, assume by way of contradiction that P is a (proper) Sylow p -subgroup of K . By the Frattini argument, $G = KN_G(P)$. Let $L := K \cap N_G(P)$; this is a normal subgroup of $N_G(P)$ and

$$N_G(P)/L \cong KN_G(P)/K \cong G/K \cong G_\alpha.$$

As $(|L|, |N_G(P)/L|) = 1$, the Schur-Zassenhaus theorem ensures the existence of a complement H for L in $N_G(P)$. Since $|H| = |N_G(P)/L| = |G_\alpha|$, the same theorem tells us that H is conjugate to G_α , so that $H = G_\beta$ for some β .

Now $G_\beta < N_G(P)$ means that if $N_G(P)$ is a proper subgroup of G , G_β (which is properly included in $N_G(P)$, for instance because $P < N_G(P)$) is not maximal, contradicting the primitivity of G . On the other hand, if $N_G(P) = G$, then P is a proper subgroup of K , which is normal in G , which contradicts K is a minimal normal subgroup. \diamond

The following propositions lead to a result which connects, in a group

with a normal regular subgroup, the Parker vector of the point stabiliser to the Parker vector of the whole group, adding to the more general results of section 2.2.

Proposition 3.2.2 *Let G be a permutation group with a normal regular subgroup K . Let g be a fixed point free element in $G \setminus K$. Then $(o(g), |K|) \neq 1$.*

Proof If not, let $H := K \langle g \rangle$. So both H_α and (by Schur-Zassenhaus theorem) $\langle g \rangle$ are complements of K in H . Therefore, there exists a β such that $\langle g \rangle = H_\beta$, so that g fixes β , contradicting the hypothesis. \diamond

Proposition 3.2.3 *Let G and K be as in Proposition 3.2.2, with $|K| = p^n$. Let $h, k \in G$. Then, for all $\alpha \in \Omega$: $[k, h] = 1$, $o(k) = p$, $(o(k), o(h)) = 1$ if, and only if: $k \in K$, $h \in G_{\alpha\beta}$ with $\alpha^k = \beta$.*

Proof (\Rightarrow) Since $o(k) = p$, $k \in K$, as K is the unique Sylow p -subgroup of G ; by the previous proposition, $h \in G_\beta$ for some β .

For h and k to commute, k has to fix setwise the set of fixed points of h . So h has to fix at least p points, which form a cycle of k .

(\Leftarrow) More or less obvious ($k^h = k'$ such that $\alpha^{k'} = \alpha^{kh} = \beta^h = \beta \Rightarrow k' = k$).

\diamond

Corollary 3.2.2 *$k \in K$ implies $C_G(k) = K \cdot G_{\alpha\beta}$ with $\alpha^k = \beta$.*

Proposition 3.2.4 *Let G and K be as in the previous propositions. Let $h \in G$, $k \in K \setminus \{1\}$, $\alpha \in \Omega$. Then:*

$$[k, h] = 1, \quad (|K|, o(h)) = 1 \quad \text{if, and only if,} \quad h \in G_{\alpha\beta} \text{ with } \alpha^k = \beta.$$

Proof The proof goes along the lines of that of the previous proposition, considering, instead of p , the least divisor of $|K|$ different from 1. \diamond

Before the next proposition, let us recall a standard fact from group theory. Let g be an element of a group, and let $o(g) = ab$ with $(a, b) = 1$. Then we can write g as a product of two commuting elements, having orders a and b . In fact, there exist integers x and y such that $ax + by = 1$; so, $g = g^{ax+by} = g^{ax}g^{by}$. The orders of the factors are as required, and they commute being powers of the same element.

Proposition 3.2.5 *Let G be a permutation group with a normal regular subgroup K . Let $K \cong C_p \times C_p$ and $(|G_\alpha|, |K|) = 1$. Then*

$$p_p(G) = p_1(G_\alpha).$$

Proof

$$\begin{aligned} p_p(G) &= \frac{1}{|G|} \sum_{g \in G} |\{c : c \text{ cycle of an element of } G; l(c) = p; c^g = c\}| \\ &= \frac{1}{|G|} \sum_{g \in G} (|\{c : c \text{ as above, in } K\}| + |\{c : c \text{ as before, in } G_\alpha\}| \\ &\quad + |\{c : c \text{ as before, in a fixed point free element of } G \setminus K\}| \\ &\quad - |\{c : c \text{ a cycle being counted more than once}\}|) \end{aligned}$$

Of these four summands, the second one is 0, because of the hypothesis $(|G_\alpha|, |K|) = 1$.

The third and the fourth cancel out. In fact, let c be a p -cycle occurring in \bar{g} , a fixed point free element in $G \setminus K$. Now, $o(\bar{g}) = pr$, $r > 1$, p not dividing r . So, by the preceding remark, $\bar{g} = kg$, with $[k, g] = 1$, $o(k) = p$ (which

divides $|K|$), and $o(g) = r$ (which divides $|G_\alpha|$). Then, by Proposition 3.2.3, $k \in K$, $g \in G_{\alpha\alpha^k}$, and g fixes exactly p points. These points form a cycle of k , which is also a cycle of \bar{g} , the unique p -cycle of \bar{g} , since the d -cycles of g , for $d > 1$, give rise to pd -cycles of \bar{g} . So each p -cycle of a fixed point free element in $G \setminus K$ is also a cycle of an element of K , and so already taken into account for.

Hence:

$$\begin{aligned}
p_p(G) &= \frac{1}{|G|} |\{(c, g) : c \text{ } p\text{-cycle of } K, c^g = c\}| \\
&= \frac{1}{|G|} \sum_{k \in K \setminus \{1\}} |C_G(k)| \\
&= \frac{1}{|G|} \sum_{k \in K \setminus \{1\}} |K \cdot G_{\alpha\beta}| \quad \text{with } \alpha^k = \beta, \text{ by Corollary 3.2.2} \\
&= \frac{|K|}{|G|} \sum_{\beta \in \Omega \setminus \{\alpha\}} |G_{\alpha\beta}| \\
&= \frac{1}{|G_\alpha|} \sum_{\beta \in \Omega \setminus \{\alpha\}} \frac{|G_\alpha|}{|\beta^{G_\alpha}|} \\
&= \sum_{\beta \in \Omega \setminus \{\alpha\}} \frac{1}{|\beta^{G_\alpha}|} \\
&= \text{number of orbits of } G_\alpha \text{ on } \Omega \setminus \{\alpha\} = p_1(G_\alpha).
\end{aligned}$$

◇

The next proposition holds in general when G splits over a normal subgroup A ; so, in particular, it holds taking as A a normal regular subgroup.

Proposition 3.2.6 *If G splits over A with B as a complement and $(k, |A|) = 1$, then $p_k(G) \leq p_k(B)$.*

Proof Assume that $g \in G$ has a k -cycle. Let n be the product of the maximum powers of the primes dividing $|A|$, dividing $|G|$. Thus, there exist

integers x, y such that $kx + ny = 1$, and $g = g^{kx} g^{ny}$. As g^{kx} fixes pointwise the k -cycles of G , g^{ny} has the same k -cycles as g .

By applying Schur-Zassenhaus theorem to $A\langle g^{ny} \rangle$, we find that $\langle g^{ny} \rangle$ is conjugated to each complement of A , so that we can assume that $g^{ny} \in B$.

So, each k -cycle occurring in G is a cycle of B . ◇

Chapter 4

Pólya enumeration

4.1 Cycle index and Pólya's theory

The notion of cycle index and the fundamental Pólya enumeration theorem are the basis for the so-called Pólya's theory of counting. We shall only marginally use it, and so are going to recall just the concepts necessary for what follows.

Definition Given a permutation group G of degree n , and denoting, as before, by $c_k(g)$ the number of k -cycles of an element g , the *cycle index* of G is the polynomial $Z(G; x_1, x_2, \dots, x_n)$ in n variables x_1, \dots, x_n defined by

$$Z(G; x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{c_1(g)} x_2^{c_2(g)} \dots x_n^{c_n(g)}.$$

When no confusion may arise, it will simply be denoted by $Z(G)$.

The cycle index may be considered as the generating function for the cycle structure of the elements of G . The standard references about it are the historical paper by Pólya ([Pó37]), and [Br64].

Let us give some examples. The cycle index for C_n in its regular action

is

$$Z(C_n) = \frac{1}{n} \sum_{k|n} \varphi(k) x_k^{n/k}.$$

This gives also the “first half” of the cycle index of the dihedral group D_n :

$$Z(D_n) = \frac{1}{2n} \sum_{k|n} \varphi(k) x_k^{n/k} + \begin{cases} \frac{1}{2} x_1 x_2^m & \text{if } n \text{ is odd, } n = 2m - 1 \\ \frac{1}{4} (x_1^2 x_2^{m-1} + x_2^m) & \text{if } n \text{ is even, } n = 2m \end{cases}.$$

Next, as the number of elements $g \in S_n$ such that $(c_1(g), c_2(g), \dots, c_n(g)) = (a_1, \dots, a_n)$ (with $\sum_i i a_i = n$) is equal to $n! / 1^{a_1} a_1! 2^{a_2} a_2! \dots n^{a_n} a_n!$, the cycle index of S_n is:

$$Z(S_n) = \sum_{(a_1, \dots, a_n)} \frac{x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}}{a_1! 2^{a_2} a_2! \dots n^{a_n} a_n!}, \quad (4.1)$$

where the sum is over all the n -tuples such that $\sum_i i a_i = n$. A concise and elegant way to put this, consists in writing out the generating function $F(z, x_1, x_2, x_3, \dots)$ of the cycle indices of the symmetric groups:

$$F(z, x_1, x_2, x_3, \dots) = \exp \left(z x_1 + \frac{z^2 x_2}{2} + \frac{z^3 x_3}{3} + \dots \right).$$

In other words, $Z(S_n; x_1, x_2, \dots)$ is equal to the coefficient of z^n in the expansion of F into a power series, which can be written as

$$\sum_{a_1=0}^{\infty} \frac{(z x_1)^{a_1}}{a_1!} \sum_{a_2=0}^{\infty} \frac{(z x_2)^{a_2}}{a_2! 2^{a_2}} \dots.$$

Unfortunately, the knowledge of the cycle index of a group does not always imply the knowledge of the group. For instance, for all odd primes p , there exist two non isomorphic groups of order p^3 such that each element has exponent p : the elementary abelian group of order p^3 and the group of

matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

over $GF(p)$ (or, equivalently, the group of triples (a, b, c) of elements of $GF(p)$, with the binary operation $(a, b, c) * (\alpha, \beta, \gamma) := (a + \alpha, b + \beta + a\gamma, c + \gamma)$).

So, of course, in their regular actions, these two groups have the same cycle index: $Z(G) = (1/p^3)(x_1^{p^3} + (p^3 - 1)x_p^2)$.

For what follows we will need the following binary operation (as defined in [Ha58]) on polynomials in variables indexed by natural numbers. It will be mainly useful when applied to cycle indices of groups, as we shall show. We shall denote this operation by \otimes and define it on variables by

$$x_i^{j_i} \otimes x_l^{k_l} := x_{\text{lcm}(i,l)}^{j_i k_l \text{gcd}(i,l)};$$

on monomials by

$$\left(\prod_{i=1}^n x_i^{j_i} \right) \otimes \left(\prod_{l=1}^m x_l^{k_l} \right) := \prod_{i=1}^n \prod_{l=1}^m x_i^{j_i} \otimes x_l^{k_l};$$

on polynomials by

$$\left(\sum_{(j)} a_{(j)} \prod_{i=1}^n x_i^{j_i} \right) \otimes \left(\sum_{(k)} b_{(k)} \prod_{l=1}^m x_l^{k_l} \right) := \sum_{(j)} \sum_{(k)} a_{(j)} b_{(k)} \left(\prod_{i=1}^n x_i^{j_i} \right) \otimes \left(\prod_{l=1}^m x_l^{k_l} \right). \quad (4.2)$$

We can now state some important properties of the cycle index.

Proposition 4.1.1 *If G and H are permutation groups, acting respectively on Ω and Δ , then*

1) *considering the action of $G \times H$ on $\Omega \times \Delta$:*

$$Z(G \times H) = Z(G) \otimes Z(H);$$

2) considering the action of $G \wr H$ on $\Omega \times \Delta$:

$$\begin{aligned} Z(G \wr H; x_1, x_2, x_3, \dots) &= \\ &= Z(H; Z(G; x_1, x_2, x_3, \dots), Z(G; x_2, x_4, x_6, \dots), \dots, Z(G; x_i, x_{2i}, x_{3i}, \dots) \dots). \end{aligned}$$

The first of these results can be found in [Ha58] and [HH68]); the second one dates back to Pólya ([P637], where he denotes by the “Kranz” $\mathcal{G}[\mathcal{H}]$ the group $H \wr G$; see also [Br64]).

Let us now briefly study the behaviour of the operation \otimes with respect to derivation; the use of this will be clear in the next section.

As a consequence of the definition of \otimes , we have:

$$s \frac{\partial}{\partial x_s} (x_i^{j_i} \otimes x_l^{k_l}) = \begin{cases} 0 & \text{if } s \neq \text{lcm}(i, l) \\ j_i k_l i l (x_i^{j_i} \otimes x_l^{k_l}) x_s^{-1} & \text{if } s = \text{lcm}(i, l) \end{cases} \quad (4.3)$$

Proposition 4.1.2

$$s x_s \frac{\partial}{\partial x_s} (x_r^a \otimes x_t^b) = \begin{cases} 0 & \text{if } s \neq \text{lcm}(r, t) \\ (r x_r \frac{\partial}{\partial x_r} x_r^a) \otimes (t x_t \frac{\partial}{\partial x_t} x_t^b) & \text{if } s = \text{lcm}(r, t) \end{cases} \quad .$$

This is just a reformulation of (4.3), but it generalises to the following, less trivial, property.

Proposition 4.1.3 *If M and N are two monomials in the variables x_j ($j = 1 \dots, k$), then:*

$$s x_s \frac{\partial}{\partial x_s} (M \otimes N) = \sum_{\substack{(a,b) \\ \text{lcm}(a,b)=s}} \left[\left(a x_a \frac{\partial}{\partial x_a} M \right) \otimes \left(b x_b \frac{\partial}{\partial x_b} N \right) \right].$$

Proof Just calculations. Let $M = \prod_{i=1}^n x_{r_i}^{j_i}$ and $N = \prod_{l=1}^m x_{t_l}^{k_l}$. Then

$$s x_s \frac{\partial}{\partial x_s} \left[\left(\prod_{i=1}^n x_{r_i}^{j_i} \right) \otimes \left(\prod_{l=1}^m x_{t_l}^{k_l} \right) \right] = s x_s \frac{\partial}{\partial x_s} \left[\prod_{i=1}^n \prod_{l=1}^m (x_{r_i}^{j_i} \otimes x_{t_l}^{k_l}) \right]$$

$$\begin{aligned}
&= \sum_{i,l} \left(s x_s \frac{\partial}{\partial x_s} (x_{r_i}^{j_i} \otimes x_{t_l}^{k_l}) \cdot \prod_{\substack{\bar{i}, \bar{l} \\ (i,l) \neq (i,l)}} (x_{r_{\bar{i}}}^{j_{\bar{i}}} \otimes x_{t_{\bar{l}}}^{k_{\bar{l}}}) \right) \\
&= \sum_{\substack{i,l \\ s=\text{lcm}(r_i, t_l)}} r_i j_i t_l k_l M \otimes N.
\end{aligned}$$

On the other hand, for any a and b ,

$$\begin{aligned}
a x_a \frac{\partial M}{\partial x_a} \otimes b x_b \frac{\partial N}{\partial x_b} &= \sum_{i=1}^n \left(a x_a \frac{\partial}{\partial x_a} x_{r_i}^{j_i} \prod_{\bar{i} \neq i} x_{r_{\bar{i}}}^{j_{\bar{i}}} \right) \otimes \sum_{l=1}^m \left(b x_b \frac{\partial}{\partial x_b} x_{t_l}^{k_l} \prod_{\bar{l} \neq l} x_{t_{\bar{l}}}^{k_{\bar{l}}} \right) \\
&= \sum_{\substack{i \\ a=r_i}} a j_i M \otimes \sum_{\substack{l \\ b=t_l}} b k_l N \\
&= \left(a \sum_{\substack{i \\ a=r_i}} j_i \right) M \otimes \left(b \sum_{\substack{l \\ b=t_l}} k_l \right) N \\
&= \left(a b \sum_{\substack{i,l \\ a=r_i, b=t_l}} j_i k_l \right) M \otimes N.
\end{aligned}$$

Summing such terms over all pairs (a, b) such that $\text{lcm}(a, b) = s$ yields the last term of the previous chain of equalities, and the statement. \diamond

By further generalising, we get the next proposition.

Proposition 4.1.4 *If p_i ($i = 1, \dots, n$) are polynomials in the variables x_j , ($j = 1, \dots, k$), then*

$$s x_s \frac{\partial}{\partial x_s} \bigotimes_{i=1}^n p_i(x_1, \dots, x_k) = \sum_{\substack{(a_1, \dots, a_n) \\ \text{lcm}(a_1, \dots, a_n) = s}} \bigotimes_{i=1}^n \left(a_i x_{a_i} \frac{\partial}{\partial x_{a_i}} p_i(x_1, \dots, x_k) \right).$$

4.2 Links with Parker vectors

The knowledge of the cycle index of a permutation group implies the knowledge of its Parker vector. More precisely, the following result holds.

Proposition 4.2.1 *If G is a permutation group then, with the usual notation,*

$$p_k(G) = k \left(\frac{\partial}{\partial x_k} Z(G) \right) \Big|_{x_i=1 \forall i}.$$

Proof The proof is straightforward:

$$\frac{\partial}{\partial x_k} Z(G) = \frac{1}{|G|} \sum_{g \in G} c_k(g) x_1^{c_1(g)} \dots x_{k-1}^{c_{k-1}(g)} x_k^{c_k(g)-1} x_{k+1}^{c_{k+1}(g)} \dots x_n^{c_n(g)};$$

hence,

$$k \left(\frac{\partial}{\partial x_k} Z(G) \right) \Big|_{x_i=1 \forall i} = \frac{1}{|G|} \sum_{g \in G} k c_k(g) = p_k(G),$$

by Parker's lemma. ◇

The already mentioned groups $C_2 \wr C_3$ and $C_3 \wr C_2$ provide an example of two groups with equal Parker vectors (as already seen) but different cycle indices (for instance, because in $C_3 \wr C_2$ elements with a single 3-cycle appear, whereas in $C_2 \wr C_3$ 3-cycles come in pairs).

The previous proposition, together with some properties of the cycle index, provides us with a method to tackle several problems in the Parker vector theory.

For instance, we can now prove the second and third claim of proposition 1.2.1.

Proof of Prop. 1.2.1, (2.) Now, let $Z_1 = Z(G, \Omega) = \sum_{(j)} a_{(j)} \prod_{i=1}^n x_i^{j_i}$ and $Z_2 = Z(H, \Delta) = \sum_{(k)} b_{(k)} \prod_{i=1}^m x_i^{k_i}$.

$$p_s(G \times H) = s \frac{\partial}{\partial x_s} Z(G \times H) \Big|_{x_i=1}$$

$$= sx_s \frac{\partial}{\partial x_s} Z(G) \otimes Z(H) \Big|_{x_i=1} \quad \text{by Prop. 4.1.1} \quad (4.4)$$

$$= \sum_{\substack{(a,b) \\ \text{lcm}(a,b)=s}} ax_a \frac{\partial Z(G)}{\partial x_a} \otimes bx_b \frac{\partial Z(H)}{\partial x_b} \Big|_{x_i=1}, \quad (4.5)$$

this last equality being justified by Prop. 4.1.4. (We remark that in (4.4) the insertion of x_s is made possible by the fact that we are evaluating everything at $x_i = 1$, for all i .)

On the other hand,

$$\sum_{\substack{(a,b) \\ \text{lcm}(a,b)=s}} p_a(G)p_b(H) = \sum_{\substack{(a,b) \\ \text{lcm}(a,b)=s}} a \frac{\partial}{\partial x_a} Z(G) \Big|_{x_i=1} b \frac{\partial}{\partial x_b} Z(H) \Big|_{x_i=1}.$$

The last term is equal to (4.5) because the definition 4.2 of \otimes on the polynomials is formally identical to the definition of the standard product, so that by setting all monomials equal to 1 we get the same result.

(3.) Again by the previous proposition,

$$\begin{aligned} p_k(G \wr H) &= k \left(\frac{\partial}{\partial s_k} Z(G \wr H) \right) \Big|_{x_i=1} \\ &= k \left(\frac{\partial}{\partial x_1} Z(G) \cdot \frac{\partial}{\partial x_k} Z(H; x_1, x_2, x_3, \dots) + \right. \\ &\quad \left. + \frac{\partial}{\partial x_2} Z(G) \cdot \frac{\partial}{\partial x_k} Z(H; x_2, x_4, x_6, \dots) + \dots \right) \Big|_{x_i=1} \\ &= k \sum_{i=1}^n \left(\frac{\partial}{\partial x_i} Z(G; x_1, x_2, x_3, \dots) \cdot \frac{\partial}{\partial s_k} Z(H; x_i, x_{2i}, x_{3i}, \dots) \right) \Big|_{x_i=1} \\ &= k \sum_{i|k} \left(\frac{1}{i} p_i(G) \frac{\partial}{\partial x_{k/i}} Z(H; x_1, x_2, x_3, \dots) \right) \Big|_{x_i=1} \quad (4.6) \\ &= k \sum_{i|k} \left(\frac{1}{i} p_i(G) \cdot \frac{i}{k} p_{k/i}(H) \right) \\ &= \sum_{i|k} p_i(G) p_{k/i}(H), \end{aligned}$$

as was to be shown. In particular, the passage (4.6), is justified by the fact that $\partial/\partial x_k Z(H; x_i, x_{2i}, x_{3i}, \dots)$ is equal to zero when i does not divide k . \diamond

A by-product of the relationship between Pólya cycle indices and Parker vectors is a curious and perhaps new identity.

If n is any fixed positive integer and k is in $\{1, 2, \dots, n\}$, then

$$k \sum_{(a)} \left(a_k \prod_{i=1}^n \frac{1}{a_i! i^{a_i}} \right) = 1, \quad (4.7)$$

where the summation is over the partitions $(a) = (a_1, \dots, a_n)$ of n : $a_1 + 2a_2 + 3a_3 + \dots = n$. The equality is obtained by equating the known value of $p_k(S_n)$, i.e. 1, to the expression for it given by applying Prop. 4.2.1 to (4.1), the cycle index of S_n .

It is related to the well-known Cauchy identity

$$\sum_{(a)} \prod_{i=1}^n \frac{1}{a_i! i^{a_i}} = 1,$$

which in this context has the trivial interpretation that by taking the permutations with all possible cycle structures, we get all of them. Analogously, (4.7) says that in the symmetric group S_n the number of all k -cycles (counting each every time it appears) is $n!/k$. Indeed, by multiplying both sides of (4.7) by $n!/k$, we count, on the left hand side, each element of S_n a number of times equal to the number of its k -cycles.

4.3 Vector space cycle index and vector space Parker vectors

It is interesting to mention a possible extension of the definition and use of cycle indices, from permutation groups to linear groups, due to J.P.S. Kung. We give after that a tentative approach to an analogue extension of Parker vectors.

Kung in [Ku81] defines a vector space analogue of the Pólya cycle index. Before recalling his definitions and working with them, let us give an outline of the general spirit of such an approach.

A group G of permutations on a set Ω can be naturally extended to a group G of automorphisms of a vector space V (linear bijective transformations onto itself), where V is the space on a fixed field k , with Ω as a basis. With respect to this basis, the elements of G correspond to permutation matrices (matrices with exactly one 1 on each row and column, and 0's elsewhere).

In this particular case, we can freely transfer the concepts and the lexicon of permutation groups to (these) linear groups, and vice versa. For instance, one could compute the characteristic polynomial of a permutation, and so on.

But we would like such a transfer to be possible in a more general situation, and this is indeed the case, somehow at least. (It is important to note that this is different from studying a linear group as the permutation group on the elements of the vector space on which it acts. This is what we shall

do in the next chapter.)

We can (informally) give a correspondence as follows:

| Permutation groups | Linear groups |
|--|--|
| $ \Omega = d$ | $\dim V = d$ |
| π permutation of Ω | α automorphism of V |
| π cyclic permutation | α cyclic automorphism (that is, one for which a vector v exists such that $\{v, v^\alpha, v^{\alpha^2}, \dots, v^{\alpha^{d-1}}\}$ is a basis of V) |
| derangement (fixed point free element) | automorphism with no invariant 1-dimensional subspaces |

Let us proceed to the formal definitions.

If $p(x) = c_0 + c_1x + \dots + c_{m-1}x^{m-1} + x^m$ is an irreducible polynomial, we

denote by γ its *companion matrix* $\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ -c_0 & & & & -c_{m-1} \end{pmatrix}$ and by $\gamma^{(t)}$

the block matrix $\begin{pmatrix} \gamma & & & & \\ \delta & \gamma & & & 0 \\ & \delta & \ddots & & \\ & & \ddots & \ddots & \\ 0 & & & \delta & \gamma \end{pmatrix}$ where $\delta = e_{1m}$ is the matrix with 1

in the m -th position of the first row, and zeros elsewhere. If b is a sequence of nonnegative integers with finitely many nonzero terms, $b = (b_1, b_2, \dots)$, let $D(p, b) = \text{diag}(\gamma^{(1)}, \dots, \gamma^{(1)}, \gamma^{(2)}, \dots, \gamma^{(2)}, \dots, \gamma^{(i)}, \dots, \gamma^{(i)}, \dots)$ with $\gamma^{(j)}$ appearing b_j times. Let \mathbf{B} be the set of all such sequences b .

If $\alpha \in GL(V)$ has characteristic polynomial p^j , with irreducible monic p , for some basis of V and some partition $b \vdash j$ (in the sense that $b_1 + 2b_2 + 3b_3 + \dots = j$), α has matrix $D(p, b)$ and this is a decomposition of α in cyclic automorphisms. This decomposition is not uniquely determined, but

the sequence b (called *species* of α) is.

For any $\alpha \in GL(V)$ with characteristic polynomial p , the factorisation of p in irreducible factors, $p(x) = p_1^{j_1}(x) \dots p_n^{j_n}(x)$, uniquely induces a decomposition of $\alpha = \bigoplus_{i=1}^n \alpha_i$, called *primary decomposition*, such that α_i acts on $V_i = \ker(p_i^{j_i}(\alpha))$, with characteristic polynomial $p_i^{j_i}$.

We can define the array $a_{i,b}(\alpha)$ ($i \in \mathbf{N}^+$, b sequence as above, $\alpha \in GL(V)$) as:

$a_{i,b}(\alpha) =$ number of summands in the primary decomposition of α having as characteristic polynomial a power of an irreducible polynomial of degree i , and species b .

The array (with finitely many nonzero entries) $a_{i,b}(\alpha)$ is called the *type* of α .

At this point, we can define the vector space cycle index of a finite group $G < GL(V)$:

$$Z(G; x) := \frac{1}{|G|} \sum_{\alpha \in G} \prod_{\substack{i > 0 \\ b \in \mathbf{B}}} x_{i,b}^{a_{i,b}(\alpha)}.$$

Now we would like to define a vector space analogue of Parker vectors. Unfortunately, there seem to be more than one “obvious” way to do so, and they do not, in general, coincide.

We can just define p_k^V to be the number of orbits of G on the cyclic automorphisms of k -dimensional subspaces of V , on which G acts as follows. If $U \subset V$ is a subspace, $\alpha : U \rightarrow U$ is a cyclic automorphism, $g \in G$ and $u \in U$, define

$$\alpha^g : U^g \rightarrow U^g, \quad (u^g)^{\alpha^g} := (u^\alpha)^g.$$

It is straightforward to see that this is indeed an action, and it is an exact analogue of the action of a permutation group on its cycles. It can be

equivalently reformulated as

$$v^{\alpha^g} := ((v^{g^{-1}})^\alpha)^g,$$

so that α^g can, as customary, be interpreted as a conjugation.

In the statement of Parker’s lemma the numbers $c_i(g)$ appear which, we recall, count the i -cycles appearing in g . Here the “natural” analogue seems to be given by the numbers $\tilde{c}_i(\alpha)$, where $\tilde{c}_i(\alpha)$ is defined as the number of cyclic automorphisms of i -dimensional subspaces of V induced by α . These numbers can be deduced from the entries of $\mathbf{a}(\alpha)$. Indeed, $a_{i,b}(\alpha)$ can be interpreted as the number of automorphisms in the primary decomposition of α , having b_1 cyclic i -dimensional subspaces, \dots , b_l cyclic li -dimensional subspaces, \dots . So, we get

$$\tilde{c}_i(\alpha) = \sum_{k|i} \sum_{b \in \mathbf{B}} a_{k,b}(\alpha) b_{i/k}.$$

Alternatively, one could just take the $a_{i,b}(\alpha)$ ’s in place of the $c_i(g)$ ’s, and define

$$p_{i,\bar{b}} := \frac{1}{|G|} \sum_{\alpha \in G} i a_{i,\bar{b}}(\alpha),$$

“paraphrasing” Parker’s lemma, and this is precisely what we get by partially deriving the (Kung) cycle index:

$$p_{i,\bar{b}} = i \left(\frac{\partial}{\partial x_{i,\bar{b}}} Z(G; x_{j,b}) \right) \Big|_{x_{j,b}=1}.$$

These numbers are not in general integers, so they cannot have an immediate combinatorial interpretation. For instance, by using the formulae given

by Kung for the (ordinary) generating function of the vector space cycle indices of the general linear groups $GL(n, q)$, one finds that $Z(GL(2, 3); x)$ is the coefficient of u^2 in

$$\left(1 + \frac{x_{1,(1)}}{c_1((1))}u + \left(\frac{x_{1,(2)}}{c_1((2))} + \frac{x_{1,(0,1)}}{c_1((0,1))}\right)u^2 + \dots\right)^2 \cdot \left(1 + \frac{x_{2,(1)}}{c_2((1))}u^2 + \dots\right)^3 \dots$$

where the dots denote higher degree terms, which do not contribute to 2nd degree term, by (1) we mean $(1, 0, \dots)$ etc., and $c_i(b)$ is the number of invertible matrices commuting with the block matrix $D(p, b)$. Thus,

$$\begin{aligned} Z(GL(2, 3); x) &= \frac{x_{1,(1)}^2}{c_1((1))^2} + 2\frac{x_{1,(2)}}{c_1((2))} + 2\frac{x_{1,(0,1)}}{c_1((0,1))} + 3\frac{x_{2,(1)}}{c_2((1))} \\ &= \frac{x_{1,(1)}^2}{4} + \frac{x_{1,(2)}}{24} + \frac{x_{1,(0,1)}}{3} + \frac{3}{8}x_{2,(1)}. \end{aligned}$$

So we obtain the “vector space Parker vector” of $GL(2, 3)$ as

$$\begin{aligned} p_{1,(1)}(GL(2, 3)) &= \frac{1}{2}, \\ p_{1,(2)}(GL(2, 3)) &= \frac{1}{24}, \\ p_{1,(0,1)}(GL(2, 3)) &= \frac{1}{3}, \\ p_{2,(1)}(GL(2, 3)) &= \frac{3}{4}, \end{aligned}$$

and all other $p_{i,b}$'s equal to zero.

Chapter 5

Linear and affine groups

A particular case of a group with a regular subgroup is given by the affine groups, in which the translations form a regular normal subgroup, and the point stabiliser is the corresponding linear group. The translation group is isomorphic to the additive group of the corresponding vector space, and so it is an elementary abelian group; it is isomorphic to $C_p \times C_p \times \dots \times C_p$ (n times) if we are considering the n -dimensional space over the field with p elements (p prime).

As we shall see, the particular structure of the affine and linear groups makes possible to get much more precise results than in the general case of groups with a regular subgroup.

So let us examine what is possible to say about the Parker vectors of the finite linear groups.

5.1 Parker vectors of general linear groups

We give a procedure to find the Parker vector of the general linear group $GL(n, q)$, in its action on the non-zero vectors of $GF(q)^n$, where q is a prime power, and to give an explicit representative for each orbit.

Theorem 5.1.1 *Let p_k be the number of square $d \times d$ matrices of the form*

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ a_0 & & \dots & & a_{d-1} \end{pmatrix} \quad (5.1)$$

with entries from $GF(q)$, $a_0 \neq 0$, d less than or equal to n , and (multiplicative) order equal to k . For $d = 1$, take all “ 1×1 matrices” (a), $a \in GF(q)^$. Then $(p_1, p_2, \dots, p_{q^n-1})$ is the Parker vector of $GL(n, q)$ in its action on $GF(q)^n \setminus \{0\}$.*

Taking a longest cycle from each such matrix (written in its cycle form as a permutation of the vectors) gives a complete set of representatives for the orbits of $GL(n, q)$ on \mathcal{C} (the set of its cycles).

The proof consists of the following remarks and lemmas. We are going to determine the Parker vector of $GL(n, q)$ by an inductive argument (on n).

1. $GL(1, q) \cong C_{q-1}$, so that its Parker vector is known.
2. Call *rank* of a cycle of an element of $GL(n, q)$ the dimension of the vector subspace generated by the vectors appearing in it, and denote

the rank of a cycle γ by $\text{rk}\gamma$. Call *rank* of an element the maximum rank of its cycles.

Obviously, two conjugate cycles have the same rank. So “being conjugate”, as an equivalence relation, is a refinement of “having the same rank” (as well as of “having the same length”).

3. It suffices to Parker-classify the maximum rank cycles in $GL(n, q)$, and add the numbers of orbits on them to the Parker vector of $GL(n-1, q)$, in order to get the Parker vector of $GL(n, q)$.

More formally:

Lemma 5.1.1 $p(GL(n, q)) = p(GL(n-1, q)) + (s_1, \dots, s_{q^n-1})$, where s_i is the number of orbits of $GL(n, q)$ on its i -cycles of rank n .

Proof If we denote the Parker vector of $GL(n-1, q)$ and that of $GL(n, q)$ by (p_i) and (\tilde{p}_i) respectively, then what we have to show is $\tilde{p}_i|_{\text{rk}\gamma < n} = p_i|_{\text{rk}\gamma < n}$, for all i . The restriction to the subset of the cycles with rank less than n is obviously justified by the fact that $GL(n-1, q)$ does not contain cycles with rank n .

- $\tilde{p}_i|_{\text{rk}\gamma < n} \leq p_i|_{\text{rk}\gamma < n}$

This means that increasing the number of cycles of a given length does not increase the number of orbits: informally, any “new” cycle is conjugate to an “old” one.

Indeed, fix a basis $\{v_1, \dots, v_{n-1}\}$ for the space $GF(q)^{n-1}$ and extend it to a basis for $V \cong GF(q)^n$ by adding a vector v_n . Consider a cycle $\gamma = (w_1, \dots, w_k, \sum_{i \leq k} a_i w_i, \dots)$ of an element of $GL(n, q)$ such that $\text{rk} \gamma = k < n$, that is, $\{w_1, \dots, w_k\}$ are linearly independent. So, there exists an element $g \in GL(n, q)$ such that $\gamma^g = (v_1, \dots, v_k, \sum_{i \leq k} b_i v_i, \dots)$, and this is a cycle appearing in an element of $GL(n-1, q)$.

- $\tilde{p}_i|_{\text{rk} \gamma < n} \geq p_i|_{\text{rk} \gamma < n}$

We want to prove that the “new” elements do not conjugate cycles not already conjugated. By contradiction, assume

$$\gamma \not\sim_{n-1} \delta, \quad \gamma \sim_n \delta$$

for some γ, δ cycles in $GL(n-1, q)$; in other words, that there exists $g \in GL(n, q) \setminus GL(n-1, q)$ such that $\gamma^g = \delta$.

By the remarks in the first part of the proof, the subspaces generated by the vectors appearing in γ and δ may be supposed to be subspaces of $\langle v_1, \dots, v_{n-1} \rangle$. Furthermore, $\text{rk} \gamma = \text{rk} \delta$ (otherwise they cannot be conjugated anywhere). So (denoting by r their common rank):

$$\gamma \sim (v_1, \dots, v_r, w, \dots)$$

$$\delta \sim (v_1, \dots, v_r, u, \dots)$$

with $w, u \in \langle v_1, \dots, v_r \rangle$. Thus, if they are conjugated at all (that is, by an element of $GL(n, q)$), they must be so already in $GL(n-$

1, q). In fact, an element of $GL(n, q)$, restricted to an invariant subspace of dimension r , gives an element of $GL(r, q) < GL(n - 1, q)$

◇

Let us explicitly state

Corollary 5.1.2 *The first $n - 1$ components of the Parker vector of $GL(n - 1, q)$ and those of $GL(n, q)$ are equal.*

Proof This immediately follows from the previous lemma, and from the fact that, by their definition, $s_1 = \dots = s_{n-1} = 0$. ◇

4. By 3. one can consider just (the cycles appearing in the cycle structure of) matrices of the form (5.1), with $a_0 \neq 0$.

That it must be so is shown by observing that a maximum rank element in $GL(n, q)$ (that is, an element containing a cycle with rank n) can be written in the form (5.1), which is indeed a matrix mapping $e_1 \mapsto e_2, e_2 \mapsto e_3, \dots, e_{n-1} \mapsto e_n, e_n \mapsto \sum_i a_{i-1}e_i$, where $\{e_i\}$ is the canonical basis. This is a kind of canonical form for maximum rank elements. (Note the similarity of this construction with that of a rational canonical form, the main difference being that here we are interested in a less fine equivalence relation and so we use these matrices without requesting the a_i to be coefficients of an irreducible polynomial.)

5. In what follows, let $m = \deg(GL(n, q)) - \deg(GL(n - 1, q))$.

At this point, to inductively get the Parker vector of $GL(n, q)$ knowing that of $GL(n - 1, q)$, we just have to check m elements of $GL(n, q)$. In fact, by what precedes, it suffices to Parker-classify the matrices of the form (5.1) with $d = n$. The following lemma allows us to check the order of such matrices rather than their cycle lengths. Their number is exactly $q^{n-1}(q - 1) = m$; they are all non-conjugate because the characteristic polynomial of (5.1) is $x^n - \sum_{i=0}^{n-1} a_i x^i$, and they all have distinct characteristic polynomials.

Lemma 5.1.2 *If A is a maximum rank element of $GL(n, q)$ then its order is equal to the length l of its longest cycle. This is the length of the maximum rank cycles.*

Proof Let γ be a maximum rank cycle, and let l be its length. Then $o(A) \geq l$.

On the other hand, γ determines the group element in which it appears (it gives the images of the elements of a basis). So for each vector v of the vector space on which $GL(n, q)$ is acting, $A^l v = v$, because this is true for the basis vectors; hence $o(A) \leq l$. \diamond

Here a worked out calculation of the above procedure follows. Consider the group $GL(2, 3)$.

The matrices satisfying the hypotheses of the theorem are the following:

$$(1), (-1), \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

It is readily checked that their orders are 1, 2, 2, 8, 8, 4, 6, and 3, respectively. So the Parker vector of $GL(2, 3)$ is $(1, 2, 1, 1, 0, 1, 0, 2)$.

Analogously, we get for the matrices of dimension 3 the orders 3, 4 (twice), 6 (three times), 8 (four times), and 13 and 26 (four times each) which, put in “vectorial” form and added to $p(GL(2, 3))$, gives $p(GL(3, 3)) = (1, 2, 2, 3, 0, 4, 0, 6, 0, 0, 0, 0, 4, 0, \dots, 0, 4)$ (26 components).

Before closing this section, let us mention another way to compute the Parker vectors of the linear groups $GL(n, q)$. Friperinger (in [Fr97]) computes the cycle indices of the linear (and other) groups, and so it is in principle sufficient to compute the partial derivatives of the expression given there to get the Parker vectors. The difficulties are just technical, and this method is less “constructive” than the one outlined in this section. It could be interesting to compare the efficiency of the two methods, implemented as computer routines (Friperinger gives some examples of computing times with SYMMETRICA routines). Friperinger’s formula for the cycle index of $GL(n, q)$ in its action on $GF(q)^n$ gives it in terms of “ \otimes -product” (as defined here in section 4.1) of monomials in variables indexed by the exponents with which the irreducible polynomials appear in the characteristic polynomials of the corresponding matrices.

5.2 Parker vectors of other linear and affine groups

The work done in the previous section allows us to easily find the Parker vectors of other related groups, first of all the special linear groups $SL(n, q)$ and the affine groups $AGL(n, q)$.

The main point has been that the study and the classification of some particular, easily detectable, elements of $GL(n, q)$ allows us to deduce the Parker vector of the group. So, if a subgroup of $GL(n, q)$ can be defined in terms of some properties of its elements, we can try to count the matrices described in Theorem 5.1.1 with these additional properties. If we get as many matrices as the degree of the group we are investigating, we have indeed got representatives for all the orbits, by virtue of the corollary to Parker's lemma. Otherwise, further analysis is needed.

Arguments of this kind give us the next theorems.

Theorem 5.2.1 *For each $k \in \{1, 2, \dots, q^{n-1}\}$ consider the set of matrices defined in Theorem 5.1.1. Let r_k be the number of such matrices admitting 1 as an eigenvalue. Then $(r_1, r_2, \dots, r_{q^{n-1}})$ is the Parker vector of $AGL(n-1, q)$ in its action on $GF(q)^{n-1}$. The second part of the above mentioned theorem holds by substituting $AGL(n-1, q)$ for $GL(n, q)$.*

Proof The group $AGL(n-1, q)$ is isomorphic to the subgroup H of $GL(n, q)$ consisting of the matrices with block form

$$\begin{pmatrix} 1 & u \\ 0 & A \end{pmatrix}, \quad (5.2)$$

where u is an element of $GF(q)^{n-1}$ (in row form), and A is an element of $GL(n-1, q)$, having the matrix (5.2) correspond to the affine transformation $v \mapsto vA + u$. The subgroup H is of course also equivalent to $AGL(n-1, q)$ as a permutation group, with H acting on the subset $\{(1, c_1, \dots, c_{n-1})\} \subset GF(q)^n$.

The elements of H are exactly, up to equivalence, the matrices admitting 1 as an eigenvalue.

So, reasoning as in Theorem 5.1.1, we only need to Parker-classify the matrices of the form (5.1) having 1 as an eigenvalue.

We conclude by remarking that such matrices number exactly q^{n-1} . In fact, for a matrix of the form (5.1) to have an eigenvalue equal to 1, it must have $(x-1)$ as a factor of its characteristic polynomial (the coefficients of which, we recall, are just given by the entries in the last row). So, it is enough to enumerate the monic polynomials, without 0 as a root, with degree at least 1 and at most $n-1$, plus the constant 1. They are

$$1 + \sum_{i=1}^{n-1} (q-1)q^{i-1} = 1 + q^{n-1} - 1 = q^{n-1}.$$

◇

For instance, one can easily see with this method that $\mathbf{p}(AGL(2, 3)) = (1, 1, 1, 1, 0, 2, 0, 2)$.

When we try to study $SL(n, q)$ using an approach similar to the one shown, we apparently run into some difficulties, ultimately due to the fact that, unlike what happens for the other groups we have considered, an ele-

ment of $SL(n, q)$, restricted to an invariant subspace of $GF(q)^n$ of dimension d , does not give in general an element of $SL(d, q)$. So we cannot simply count matrices of a particular form of all sizes up to n . However, any element of $GL(m, q)$ ($m < n$) can be extended to an element of $SL(n, q)$. So we have to consider $\mathbf{p}(GL(n-1, q))$, that is the classification of all cycles of rank less than n , and add to it the contribute given by cycles of rank n .

To find this, consider again the matrices of the form (5.1) of dimension n , with the added requisite for the determinant to be 1 that is, for a_0 to be $(-1)^{n+1}$.

Now, for each cycle $(v_1, v_2, \dots, v_n, \sum a_i v_{i+1}, \dots)$ appearing in a permutation corresponding to one of these matrices, we have $q-1$ non-conjugate cycles (including it):

$$(v_1, v_2, \dots, v_{n-1}, bv_n, (-1)^{n+1}v_1 + \sum_{i=1}^{n-2} a_i v_{i+1} + a_{n-1}bv_n, \dots),$$

$(b \in GF(q) \setminus \{0\})$.

In fact, an element conjugating

$$(v_1, v_2, \dots, v_{n-1}, bv_n, (-1)^{n+1}v_1 + \sum_{i=1}^{n-2} a_i v_{i+1} + a_{n-1}bv_n, \dots)$$

and

$$(v_1, v_2, \dots, v_{n-1}, bv_n, (-1)^{n+1}v_1 + \sum_{i=1}^{n-2} a_i v_{i+1} + a_{n-1}cv_n, \dots) \quad (5.3)$$

with $b \neq c$, is either the matrix $D = \text{diag}(1, 1, \dots, 1, c/b)$ (which has deter-

minant different from 1) or D composed with some multiple of

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & c \\ \frac{(-1)^{n+1}}{c} & a_1 & \dots & & a_{d-1} \end{pmatrix},$$

the matrix which represent the cycle (5.3) and which has determinant equal to 1. In both cases the conjugating element is in $GL(n, q) \setminus SL(n, q)$. So all these cycles belong to elements with the same determinant, 1, and are all non-conjugate in $SL(n, q)$.

So, for each of the q^{n-1} possible last rows of (5.1) (those with fixed first entry equal to $(-1)^{n+1}$) we have exhibited $q - 1$ non-conjugate cycles. In all, these are $(q - 1)q^{n-1}$ non-conjugate cycles of rank n which, together with the $q^{n-1} - 1$ cycles of lesser rank already considered (the ones coming from $GL(n - 1, q)$), give a complete set of representatives for the action of $SL(n, q)$ on its cycles.

To summarise:

Theorem 5.2.2 *Let s_k be the number of matrices of the form (5.1) with dimension $d = n$, $a_0 = (-1)^{n+1}$, and (multiplicative) order equal to k . Then the k -th component of the Parker vector of $SL(n, q)$ is $p_k(SL(n, q)) = p_k(GL(n - 1, q)) + (q - 1)s_k$. The second part holds by substituting $SL(n, q)$ for $GL(n, q)$.*

For instance, as we have seen in the previous section, $p(GL(2, 3)) = (1, 2, 1, 1, 0, 1, 0, 2)$; the matrices described in the theorem, for $q = 3$ and

$n = 3$, are

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{pmatrix}$$

with orders 3, 8, 13, 13, 13, 6, 8, 4, 13, respectively; so $s_3 = s_4 = s_6 = 1$,

$s_8 = 2$, $s_{13} = 4$, the other s_i 's being 0. Thus, $\mathbf{p}(SL(3, 3)) = (1, 2, 1+2 \cdot 1, 1+2 \cdot$

$1, 0, 1+2 \cdot 1, 0, 2+2 \cdot 2, 0, \dots, 0, 0+2 \cdot 4, 0, \dots, 0) = (1, 2, 3, 3, 0, 3, 0, 6, 0, \dots, 0, 8, 0, \dots, 0)$,

with 8 in the 13th position. For the sake of completeness, $\mathbf{p}(SL(2, 3)) =$

$(1, 1, 2, 2, 0, 2, 0, 0)$.

Appendix A

GAP programs and a table of Parker vectors

None of the results in this thesis was obtained by using computer programs. Nonetheless, the computer has been used heuristically, in order to get a grasp on some concepts before studying them directly, or to get help in looking for some examples or counterexamples. So some GAP (cf. [S⁺95]) routines were written, in order to compute the Parker vector of a given group, or to get a table of the Parker vectors of several groups.

Hereafter we give a sample of these routines. This not being a work in computer science, and the author not being an expert in programming, no claim on efficiency or even good programming practice is made about them.

The following routine is just the definition of a function, `parker`, accepting as its input a permutation group and its degree and giving as output the Parker vector of the group.

The first function, `cyc`, computes $c_k(g)$, where g is an element of a group of degree `degree`.

```

cyc := function(g,degree,k)
    local f;
    f := Number(Cycles(g,[1..degree]),a->Length(a)=k);
    return f;
end;

```

The following routine, which makes use of `cyc`, is the definition of a function, `parker`, accepting as its input a permutation group and its degree and giving as output the Parker vector of the group.

```

parker := function(group,degree)
    local k, SG, vdp;
    SG := Elements(group); vdp := [];
    for k in [1..degree] do
        vdp[k] := Sum(SG,g->k*cyc(g,degree,k)/Length(SG));
    od;
    return vdp;
end

```

The crucial instruction of the function `parker` is

$$\text{vdp}[k] := \text{Sum}(\text{SG}, g \rightarrow k \cdot \text{cyc}(g, \text{degree}, k) / \text{Length}(\text{SG})),$$

which lets the k -th component of the vector be equal to the sum on all elements g of k times the number $\text{cyc}(g, \text{degree}, k) = c_k(g)$ of cycles of length k of g , divided by the order $\text{Length}(\text{SG})$ of the group; in other words, Parker's lemma.

A simple loop including the function `parker` can print out a table with the Parker vectors of all transitive groups of a prescribed range of degrees. For instance, we get the following table of all the transitive groups up to degree 10 (excluding the symmetric and alternating ones). The notation used here by GAP is the one introduced by Conway, Hulpke, and McKay in [CHM98].

DEGREE 4

$$G = C(4) = 4 \quad [1, 1, 0, 2].$$

$$G = E(4) = 2[x]2 \quad [1, 3, 0, 0].$$

$$G = D(4) \quad [1, 2, 0, 1].$$

DEGREE 5

$$G = C(5) = 5 \quad [1, 0, 0, 0, 4].$$

$$G = D(5) = 5:2 \quad [1, 2, 0, 0, 2].$$

$$G = F(5) = 5:4 \quad [1, 1, 0, 2, 1].$$

DEGREE 6

$$G = C(6) = 6 = 3[x]2 \quad [1, 1, 2, 0, 0, 2].$$

$$G = D_6(6) = [3]2 \quad [1, 3, 2, 0, 0, 0].$$

$$G = D(6) = S(3)[x]2 \quad [1, 3, 1, 0, 0, 1].$$

$$G = A_4(6) = [2^2]3 \quad [1, 1, 4, 0, 0, 0].$$

$$G = F_{18}(6) = [3^2]2 = 3 \text{ wr } 2 \quad [1, 1, 2, 0, 0, 2].$$

$$G = 2A_4(6) = [2^3]3 = 2 \text{ wr } 3 \quad [1, 1, 2, 0, 0, 2].$$

$$G = S_4(6d) = [2^2]S(3) \quad [1, 2, 2, 1, 0, 0].$$

$$\begin{aligned}
G = S_4(6c) &= 1/2[2^3]S(3) && [1, 2, 2, 1, 0, 0]. \\
G = F_{18}(6):2 &= [1/2.S(3)^2]2 && [1, 2, 1, 0, 0, 2]. \\
G = F_{36}(6) &= 1/2[S(3)^2]2 && [1, 2, 1, 2, 0, 0]. \\
G = 2S_4(6) &= [2^3]S(3) = 2 \text{ wr } S(3) && [1, 2, 1, 1, 0, 1]. \\
G = L(6) &= PSL(2,5) = A_5(6) && [1, 1, 2, 0, 2, 0]. \\
G = F_{36}(6):2 &= [S(3)^2]2 = S(3) \text{ wr } 2 && [1, 2, 1, 1, 0, 1]. \\
G = L(6):2 &= PGL(2,5) = S_5(6) && [1, 1, 1, 1, 1, 1].
\end{aligned}$$

DEGREE 7

$$\begin{aligned}
G = C(7) &= 7 && [1, 0, 0, 0, 0, 0, 6]. \\
G = D(7) &= 7:2 && [1, 3, 0, 0, 0, 0, 3]. \\
G = F_{21}(7) &= 7:3 && [1, 0, 4, 0, 0, 0, 2]. \\
G = F_{42}(7) &= 7:6 && [1, 1, 2, 0, 0, 2, 1]. \\
G = L(7) &= L(3,2) && [1, 1, 2, 1, 0, 0, 2].
\end{aligned}$$

DEGREE 8

$$\begin{aligned}
G = C(8) &= 8 && [1, 1, 0, 2, 0, 0, 0, 4]. \\
G = 4[x]2 &&& [1, 3, 0, 4, 0, 0, 0, 0]. \\
G = E(8) &= 2[x]2[x]2 && [1, 7, 0, 0, 0, 0, 0, 0]. \\
G = D_8(8) &= [4]2 && [1, 5, 0, 2, 0, 0, 0, 0]. \\
G = Q_8(8) &&& [1, 1, 0, 6, 0, 0, 0, 0]. \\
G = D(8) &&& [1, 4, 0, 1, 0, 0, 0, 2]. \\
G = 1/2[2^3]4 &&& [1, 1, 0, 2, 0, 0, 0, 4].
\end{aligned}$$

$$\begin{aligned}
G = 2D_8(8) &= [D(4)]^2 && [1, 2, 0, 3, 0, 0, 0, 2]. \\
G = E(8):2 &= D(4)[x]^2 && [1, 5, 0, 2, 0, 0, 0, 0]. \\
G &= [2^2]_4 && [1, 3, 0, 4, 0, 0, 0, 0]. \\
G = 1/2[2^3]E(4) &= Q_8:2 && [1, 3, 0, 4, 0, 0, 0, 0]. \\
G = 2A_4(8) &= [2]A(4) = SL(2,3) && [1, 1, 2, 2, 0, 2, 0, 0]. \\
G = E(8):3 &= A(4)[x]^2 && [1, 3, 2, 0, 0, 2, 0, 0]. \\
G = S(4)[1/2]^2 &= 1/2(S_4[x]^2) && [1, 3, 2, 2, 0, 0, 0, 0]. \\
G = [1/4.cD(4)^2]^2 &&& [1, 3, 0, 2, 0, 0, 0, 2]. \\
G = 1/2[2^4]_4 &&& [1, 2, 0, 1, 0, 0, 0, 4]. \\
G = [4^2]^2 &&& [1, 2, 0, 3, 0, 0, 0, 2]. \\
G = E(8):E_4 &= [2^2]D(4) && [1, 4, 0, 3, 0, 0, 0, 0]. \\
G = E(8):4 &= [1/4.eD(4)^2]^2 && [1, 3, 0, 4, 0, 0, 0, 0]. \\
G = [2^3]_4 &&& [1, 2, 0, 5, 0, 0, 0, 0]. \\
G = 1/2[2^4]E(4) &= [1/4.dD(4)^2]^2 && [1, 4, 0, 3, 0, 0, 0, 0]. \\
G = E(8):D_4 &= [2^3]2^2 && [1, 4, 0, 3, 0, 0, 0, 0]. \\
G = 2S_4(8) &= GL(2,3) && [1, 2, 1, 1, 0, 1, 0, 2]. \\
G = E(8):D_6 &= S(4)[x]^2 && [1, 3, 1, 2, 0, 1, 0, 0]. \\
G = E(8):7 &= F_56(8) && [1, 1, 0, 0, 0, 0, 6, 0]. \\
G = 1/2[2^4]eD(4) &&& [1, 3, 0, 2, 0, 0, 0, 2]. \\
G = [2^4]_4 &&& [1, 2, 0, 3, 0, 0, 0, 2]. \\
G = 1/2[2^4]dD(4) &&& [1, 3, 0, 2, 0, 0, 0, 2]. \\
G = E(8):D_8 &= [2^3]D(4) && [1, 3, 0, 4, 0, 0, 0, 0]. \\
G = 1/2[2^4]cD(4) &&& [1, 3, 0, 4, 0, 0, 0, 0].
\end{aligned}$$

$$\begin{aligned}
G &= [2^4]E(4) && [1, 4, 0, 3, 0, 0, 0, 0]. \\
G &= [2^3]A(4) && [1, 2, 2, 1, 0, 2, 0, 0]. \\
G &= E(8):A_4 = [1/3.A(4)^2]2 = E(4):6 && [1, 2, 2, 1, 0, 2, 0, 0]. \\
G &= 1/2[E(4)^2:S_3]2 = E(4)^2:D_6 && [1, 2, 2, 3, 0, 0, 0, 0]. \\
G &= [2^4]D(4) && [1, 3, 0, 3, 0, 0, 0, 1]. \\
G &= E(8):F_{21} && [1, 1, 2, 0, 0, 2, 2, 0]. \\
G &= L(8) = PSL(2,7) && [1, 1, 2, 2, 0, 0, 2, 0]. \\
G &= [2^4]A(4) && [1, 2, 2, 1, 0, 2, 0, 0]. \\
G &= [2^3]S(4) && [1, 2, 1, 3, 0, 1, 0, 0]. \\
G &= 1/2[2^4]S(4) && [1, 2, 1, 1, 0, 1, 0, 2]. \\
G &= E(8):S_4 = [E(4)^2:S_3]2 = E(4)^2:D_{12} && [1, 2, 1, 3, 0, 1, 0, 0 \\
&&&]. \\
G &= [A(4)^2]2 && [1, 2, 2, 1, 0, 2, 0, 0]. \\
G &= L(8):2 = PGL(2,7) && [1, 1, 1, 1, 0, 1, 1, 2]. \\
G &= [2^4]S(4) && [1, 2, 1, 2, 0, 1, 0, 1]. \\
G &= [1/2.S(4)^2]2 && [1, 2, 1, 2, 0, 2, 0, 0]. \\
G &= 1/2[S(4)^2]2 && [1, 2, 1, 2, 0, 0, 0, 2]. \\
G &= [S(4)^2]2 && [1, 2, 1, 2, 0, 1, 0, 1]. \\
G &= E(8):L_7 = AL(8) && [1, 1, 1, 2, 0, 1, 2, 0].
\end{aligned}$$

DEGREE 9

$$\begin{aligned}
G &= C(9) = 9 && [1, 0, 2, 0, 0, 0, 0, 0, 6]. \\
G &= E(9) = 3[x]3 && [1, 0, 8, 0, 0, 0, 0, 0, 0].
\end{aligned}$$

$$\begin{aligned}
G = D(9) = 9:2 & \quad [1, 4, 1, 0, 0, 0, 0, 0, 3]. \\
G = S(3)[x]_3 & \quad [1, 1, 5, 0, 0, 2, 0, 0, 0]. \\
G = S(3)[1/2]S(3) = 3^2:2 & \quad [1, 4, 4, 0, 0, 0, 0, 0, 0]. \\
G = 1/3[3^3]_3 & \quad [1, 0, 2, 0, 0, 0, 0, 0, 6]. \\
G = E(9):3 = [3^2]_3 & \quad [1, 0, 8, 0, 0, 0, 0, 0, 0]. \\
G = S(3)[x]S(3) = E(9):D_4 & \quad [1, 3, 3, 0, 0, 2, 0, 0, 0]. \\
G = E(9):4 & \quad [1, 2, 2, 4, 0, 0, 0, 0, 0]. \\
G = [3^2]S(3)_6 & \quad [1, 2, 1, 0, 0, 2, 0, 0, 3]. \\
G = E(9):6 = 1/2[3^2:2]S(3) & \quad [1, 2, 4, 0, 0, 2, 0, 0, 0]. \\
G = [3^2]S(3) & \quad [1, 1, 5, 0, 0, 2, 0, 0, 0]. \\
G = E(9):D_6 = [3^2:2]_3 = [1/2.S(3)^2]_3 & \quad [1, 1, 5, 0, 0, 2, 0, 0, 0 \\
& \quad]. \\
G = M(9) = E(9):Q_8 & \quad [1, 1, 1, 6, 0, 0, 0, 0, 0]. \\
G = E(9):8 & \quad [1, 1, 1, 2, 0, 0, 0, 4, 0]. \\
G = E(9):D_8 & \quad [1, 2, 2, 2, 0, 2, 0, 0, 0]. \\
G = [3^3]_3 = 3 \text{ wr } 3 & \quad [1, 0, 4, 0, 0, 0, 0, 0, 4]. \\
G = E(9):D_{12} = [3^2:2]S(3) = [1/2.S(3)^2]S(3) & \\
[1, 2, 3, 0, 0, 3, 0, 0, 0]. & \\
G = E(9):2D_8 & \quad [1, 1, 1, 3, 0, 1, 0, 2, 0]. \\
G = [3^3]S(3) = 3 \text{ wr } S(3) & \quad [1, 1, 3, 0, 0, 2, 0, 0, 2]. \\
G = 1/2.[3^3:2]S(3) & \quad [1, 2, 2, 0, 0, 2, 0, 0, 2]. \\
G = [3^3:2]_3 & \quad [1, 1, 3, 0, 0, 2, 0, 0, 2]. \\
G = E(9):2A_4 & \quad [1, 1, 3, 2, 0, 2, 0, 0, 0].
\end{aligned}$$

$$\begin{aligned}
G &= [3^3:2]S(3) && [1, 2, 2, 0, 0, 3, 0, 0, 1]. \\
G &= [1/2.S(3)^3]3 && [1, 1, 3, 0, 0, 0, 0, 0, 4]. \\
G &= E(9):2S_4 && [1, 1, 2, 1, 0, 2, 0, 2, 0]. \\
G &= L(9) = PSL(2,8) && [1, 1, 1, 0, 0, 0, 3, 0, 3]. \\
G &= [S(3)^3]3 = S(3) \text{ wr } 3 && [1, 1, 3, 0, 0, 2, 0, 0, 2]. \\
G &= [1/2.S(3)^3]S(3) && [1, 2, 2, 1, 0, 1, 0, 0, 2]. \\
G &= 1/2[S(3)^3]S(3) && [1, 2, 2, 1, 0, 1, 0, 0, 2]. \\
G &= [S(3)^3]S(3) = S(3) \text{ wr } S(3) && [1, 2, 2, 1, 0, 2, 0, 0, 1]. \\
G &= L(9):3 = P|L(2,8) && [1, 1, 1, 0, 0, 2, 1, 0, 3].
\end{aligned}$$

DEGREE 10

$$\begin{aligned}
G &= C(10) = 5[x]2 && [1, 1, 0, 0, 4, 0, 0, 0, 0, 4]. \\
G &= D(10) = 5:2 && [1, 5, 0, 0, 4, 0, 0, 0, 0, 0]. \\
G &= D_{10}(10) = [D(5)]2 && [1, 5, 0, 0, 2, 0, 0, 0, 0, 2]. \\
G &= 1/2[F(5)]2 && [1, 3, 0, 4, 2, 0, 0, 0, 0, 0]. \\
G &= F(5)[x]2 && [1, 3, 0, 4, 1, 0, 0, 0, 0, 1]. \\
G &= [5^2]2 && [1, 1, 0, 0, 4, 0, 0, 0, 0, 4]. \\
G &= A_5(10) && [1, 2, 3, 0, 4, 0, 0, 0, 0, 0]. \\
G &= [2^4]5 && [1, 1, 0, 0, 8, 0, 0, 0, 0, 0]. \\
G &= [1/2.D(5)^2]2 && [1, 3, 0, 0, 2, 0, 0, 0, 0, 4]. \\
G &= 1/2[D(5)^2]2 && [1, 3, 0, 4, 2, 0, 0, 0, 0, 0]. \\
G &= A(5)[x]2 && [1, 3, 1, 0, 2, 1, 0, 0, 0, 2]. \\
G &= 1/2[S(5)]2 = S_5(10a) && [1, 3, 1, 2, 2, 1, 0, 0, 0, 0].
\end{aligned}$$

$$\begin{aligned}
G = S_5(10d) & \quad [1, 2, 2, 2, 2, 1, 0, 0, 0, 0]. \\
G = [2^5]5 & \quad [1, 1, 0, 0, 4, 0, 0, 0, 0, 4]. \\
G = [2^4]D(5) & \quad [1, 3, 0, 2, 4, 0, 0, 0, 0, 0]. \\
G = 1/2[2^5]D(5) & \quad [1, 3, 0, 2, 4, 0, 0, 0, 0, 0]. \\
G = [5^2:4]2 & \quad [1, 2, 0, 4, 1, 0, 0, 0, 0, 2]. \\
G = [5^2:4]2_2 & \quad [1, 2, 0, 2, 1, 0, 0, 4, 0, 0]. \\
G = [5^2:4_2]2 & \quad [1, 2, 0, 2, 1, 0, 0, 0, 0, 4]. \\
G = [5^2:4_2]2_2 & \quad [1, 2, 0, 6, 1, 0, 0, 0, 0, 0]. \\
G = [D(5)^2]2 & \quad [1, 3, 0, 2, 2, 0, 0, 0, 0, 2]. \\
G = S(5)[x]2 & \quad [1, 3, 1, 2, 1, 1, 0, 0, 0, 1]. \\
G = [2^5]D(5) & \quad [1, 3, 0, 2, 2, 0, 0, 0, 0, 2]. \\
G = [2^4]F(5) & \quad [1, 2, 0, 3, 2, 0, 0, 2, 0, 0]. \\
G = 1/2[2^5]F(5) & \quad [1, 2, 0, 3, 2, 0, 0, 2, 0, 0]. \\
G = L(10) = PSL(2,9) & \quad [1, 1, 2, 2, 4, 0, 0, 0, 0, 0]. \\
G = [1/2.F(5)^2]2 & \quad [1, 2, 0, 4, 1, 0, 0, 0, 0, 2]. \\
G = 1/2[F(5)^2]2 & \quad [1, 2, 0, 2, 1, 0, 0, 4, 0, 0]. \\
G = [2^5]F(5) & \quad [1, 2, 0, 3, 1, 0, 0, 2, 0, 1]. \\
G = L(10):2 = PGL(2,9) & \quad [1, 1, 1, 1, 2, 0, 0, 2, 0, 2]. \\
G = M(10) = L(10)'2 & \quad [1, 1, 1, 3, 2, 0, 0, 2, 0, 0]. \\
G = S_6(10) = L(10):2 & \quad [1, 1, 2, 2, 2, 2, 0, 0, 0, 0]. \\
G = [F(5)^2]2 & \quad [1, 2, 0, 3, 1, 0, 0, 2, 0, 1]. \\
G = [2^4]A(5) & \quad [1, 2, 1, 1, 4, 1, 0, 0, 0, 0]. \\
G = L(10).2^2 = P|L(2,9) & \quad [1, 1, 1, 2, 1, 1, 0, 2, 0, 1].
\end{aligned}$$

```

G = [2^5]A(5)          [ 1, 2, 1, 1, 2, 1, 0, 0, 0, 2 ].
G = [2^4]S(5)         [ 1, 2, 1, 2, 2, 1, 0, 1, 0, 0 ].
G = 1/2[2^5]S(5)      [ 1, 2, 1, 2, 2, 1, 0, 1, 0, 0 ].
G = [2^5]S(5)         [ 1, 2, 1, 2, 1, 1, 0, 1, 0, 1 ].
G = [A(5)^2]2        [ 1, 2, 1, 1, 2, 1, 0, 0, 0, 2 ].
G = [1/2.S(5)^2]2 = [A(5):2]2      [ 1, 2, 1, 2, 1, 1, 0, 0, 0, 2 ].
G = 1/2[S(5)^2]2     [ 1, 2, 1, 2, 1, 1, 0, 2, 0, 0 ].
G = [S(5)^2]2       [ 1, 2, 1, 2, 1, 1, 0, 1, 0, 1 ].

```

The following function, `guess`, somehow emulates what happens in the situation described in section 1.1: it gives an estimate of the Parker vector of `group`, by randomly sampling `iterations` elements from it, and calculating the contribution they give to the vector. This is not in general an integer, so the routine gives as its output the “raw” vector so obtained, as well as the vector obtained by rounding each term to the nearest integer (rounding arbitrarily up numbers of the form $k + 1/2$, k integer).

```

guess := function(group,degree,iterations)
  local vdp, p, q, SG, k;
  vdp := []; p := []; q := []; SG := Elements(group);
  for k in [1..degree] do
    p[k] := Sum([1..iterations], a->k*cyc(Random(group),degree,k)/iterations);
    q[k] := Int(p[k] + 1/2);
  od;

```

```

    return [p,q];
end;

```

Some typical outputs of `guess`, applying it to the point stabiliser of the Suzuki group $Sz(8)$, an example of a Frobenius group with non-abelian kernel, are:

```

gap> G:=Stabilizer(PermGroup(PerfectGroup(29120)),65);;
gap> guess(G,64,200);
[ [ 299/200, 16/25, 0, 184/25, 0, 0, 2709/50, 0, ...],
  [ 1, 1, 0, 7, 0, 0, 54, 0, ...] ]
gap> guess(G,64,200);
[ [ 87/100, 8/5, 0, 232/25, 0, 0, 441/8, 0, ...],
  [ 1, 2, 0, 9, 0, 0, 55, 0, ...] ]
gap> guess(G,64,200);
[ [ 179/200, 16/25, 0, 208/25, 0, 0, 2709/50, 0, ...],
  [ 1, 1, 0, 8, 0, 0, 54, 0, ...] ]

```

(The final zeros have been deleted for clarity). The last “guess” shown is correct, as it was shown at the end of Chapter 2; we could have anyway had some “confidence” in it, by observing that, unlike what happens for the first two, in it the components of the rounded vector add up to 64, the degree of G .

Bibliography

- [AM77] Guido Almansi and Bruce Merry, *Eugenio Montale. The private language of poetry*, Edinburgh U.P., 1977.
- [Br64] N.G. de Bruijn, Pólya's Theory of Counting, pp.144–184 in *Applied Combinatorial Mathematics* (ed. Edwin F. Beckenbach), John Wiley, New York, 1964.
- [Ca98] Peter J. Cameron, *Permutation Groups*, Cambridge U.P., to appear.
- [CHM98] J.H. Conway, A. Hulpke, and J. McKay, On Transitive Permutation Groups, *LMS Journal of Computation and Mathematics* **1** (1998), 1–8 [electronic journal, located at the URL <http://www.lms.ac.uk/jcm/>].
- [DM96] John D. Dixon and Brian Mortimer, *Permutation Groups*, GTM 163, Springer, 1996.
- [Fr97] Harald Fripertinger, Cycle Indices of Linear, Affine, and Projective Groups, *Linear Algebra Appl.* **263** (1997), 133–156.

- [GS92] Robert M. Guralnick and Jan Saxl, Primitive Permutation Characters, pp. 364–367 in *Groups, Combinatorics and Geometry* (eds. Martin W. Liebeck and Jan Saxl), LMS 165, Cambridge U.P., 1992.
- [Ha58] Frank Harary, On the number of bi-colored graphs, *Pacific J. Math.* **8** (1958), 743–755.
- [HB82] B[ertram] Huppert and N[orman] Blackburn, *Finite Groups III*, Springer, 1982.
- [HH68] Michael A. Harrison and Robert G. High, On the Cycle Index of a Product of Permutation Groups, *J. Comb. Theory* **4** (1968), 277–299.
- [Is76] I. Martin Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976 [also Dover Publ., New York, 1994].
- [Ku81] Joseph P.S. Kung, The Cycle Structure of a Linear Transformation over a Finite Field, *Linear Algebra Appl.* **36** (1981), 141–155.
- [La93] Serge Lang, *Algebra* (3rd ed.), Addison-Wesley, 1993.
- [Pa68] Donald Passman, *Permutation Groups*, W.A. Benjamin, Inc., New York and Amsterdam, 1968.
- [Pó37] G[eorge] Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Mathematica* (Uppsala) **68** (1937), 145–254.

- [Ro78] John S. Rose, *A Course in Group Theory*, Cambridge U.P., 1978
[also Dover Publ., New York, 1994].
- [S+95] Martin Schönert et al. *GAP – Groups, Algorithms, and Programming*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.
- [Wi64] Helmut Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.
- [Za82] H. Zantema, Integer valued polynomials over a number field, *Manuscripta Math.* **40** (1982), 155–203.